

# SEQUENCES WITH SMALL CORRELATION

KAI-UWE SCHMIDT

**ABSTRACT.** The extent to which a sequence of finite length differs from a shifted version of itself is measured by its aperiodic autocorrelations. Of particular interest are sequences whose entries are 1 or  $-1$ , called binary sequences, and sequences whose entries are complex numbers of unit magnitude, called unimodular sequences. Since the 1950s, there is sustained interest in sequences with small aperiodic autocorrelations relative to the sequence length. One of the main motivations is that a sequence with small aperiodic autocorrelations is intrinsically suited for the separation of signals from noise, and therefore has natural applications in digital communications. This survey reviews the state of knowledge concerning the two central problems in this area: How small can the aperiodic autocorrelations of a binary or a unimodular sequence collectively be and how can we efficiently find the best such sequences? Since the analysis and construction of sequences with small aperiodic autocorrelations is closely tied to the (often much easier) analysis of periodic autocorrelation properties, several fundamental results on corresponding problems in the periodic setting are also reviewed.

## 1. INTRODUCTION

By a *sequence* of length  $n$  we mean an element of  $\mathbb{C}^n$ . For a sequence  $A$  of length  $n$ , we denote by  $A(k)$  the  $k$ -th entry in  $A$  (starting with  $k = 0$ ). It is convenient to allow  $k$  to be an arbitrary integer and reduce  $k$  modulo  $n$  if necessary. It is desirable from a practical viewpoint and appealing from a theoretical viewpoint to restrict the entries of a sequence to a small set. The most interesting case occurs when the entries are just  $-1$  or  $1$ , in which case we call the sequence *binary*.

Let  $A$  be a sequence of length  $n$ . For an integer  $u$  with  $0 \leq u < n$ , let

$$C_u(A) = \sum_{0 \leq k, k+u < n} A(k) \overline{A(k+u)}$$

be the *aperiodic autocorrelation* of  $A$  at shift  $u$ . We call  $C_0(A)$ , the sum of squared magnitudes of entries of  $A$ , the *trivial* aperiodic autocorrelation of  $A$  and the values of  $C_u(A)$  for all nonzero  $u$  the *nontrivial* aperiodic autocorrelations of  $A$ .

There is sustained interest in sequences with restricted entries such that their nontrivial aperiodic autocorrelations are small with respect to some measure. For example, Turyn [107] asked for binary sequences having the ideal property that all nontrivial aperiodic autocorrelations are in the set  $\{-1, 0, 1\}$ . Such sequences are now called *Barker sequences*, since a related problem was studied earlier by Barker [5]. The problem as to whether there exist infinitely many Barker sequences is still open, although there is overwhelming evidence that there is no Barker sequence of length greater than 13. Many of the problems discussed in this survey are motivated by the apparent nonexistence

---

*Date:* 06 October 2015.

2010 *Mathematics Subject Classification.* 94A55, 11B83, 05B10.

of long Barker sequences. The most natural question is to ask for binary sequences for which the magnitudes of the nontrivial aperiodic autocorrelations are collectively as small as possible. This problem will be discussed in Section 3.

For a sequence  $A$  of length  $n$  and an integer  $u$ , let

$$R_u(A) = \sum_{k=0}^{n-1} A(k) \overline{A(k+u)}$$

be the *periodic autocorrelation* of  $A$  at shift  $u$ . Again, we call  $R_0(A)$  the *trivial* periodic autocorrelation of  $A$  and the values of  $R_u(A)$  for all nonzero  $u$  the *nontrivial* periodic autocorrelations of  $A$ . The relationship between the aperiodic and periodic autocorrelations of a sequence  $A$  of length  $n$  is given by

$$(1.1) \quad R_u(A) = C_u(A) + \overline{C_{n-u}(A)} \quad \text{for } 0 < u < n.$$

The periodic autocorrelations are usually much easier to study than their aperiodic counterparts. Indeed, a typical attempt to obtain sequences with good aperiodic autocorrelations is to identify sequences with good periodic autocorrelations and then examine their aperiodic autocorrelations. We shall see that this approach often works well. Periodic autocorrelations also arise in settling the existence question for Barker sequences since a putative Barker sequence of length greater than 13 must have all of its nontrivial periodic autocorrelations equal to zero; such a sequence is called *perfect*. The existence of infinitely many perfect binary sequences is also still unsettled, although likewise there is overwhelming evidence that there is no perfect binary sequence of length greater than 4. While the study of periodic autocorrelations is historically at least partly motivated by questions involving aperiodic autocorrelations, many challenging problems have since arisen in the periodic case and the field has become a very active research area. Some fundamental topics will be discussed in Section 2.

The apparent nonexistence of long Barker sequences has led researchers to study alternative objects by relaxing various constraints. One possibility, discussed in Section 4, is to consider *H-phase* sequences, namely sequences whose entries are  $H$ -th roots of unity, and *unimodular* sequences, namely sequences whose entries have unit magnitude. Another possibility, discussed in Section 5, is to consider *Golay pairs*, namely pairs of sequences whose aperiodic autocorrelations sum to zero for each nonzero shift.

There are several other works that survey topics involving correlations of sequences. Like the present survey, most of them focus on particular aspects. Some recommended articles that also helped me in preparing the present survey are: Turyn [112], which covers the essential knowledge until 1968; Jungnickel and Pott [59] and Cai and Ding [16], which concentrate on optimal binary sequences and cyclic difference sets; Hellese and Kumar [47] and Golomb and Gong [41], whose focus is on periodic correlations; Jedwab [53], whose focus is on aperiodic autocorrelations; and Jedwab [52] and Høholdt [48], which survey results on the merit factor problem for binary sequences until 2006. For the interested reader, I also recommend Borwein [9], which covers some material of this survey and exhibits many interesting connections to analysis and number theory.

## 2. PERIODIC AUTOCORRELATION OF BINARY SEQUENCES

## 2.1. BOUNDS AND CONSTRUCTIONS

In this section we are interested in binary sequences for which the nontrivial periodic autocorrelations are as small as possible in magnitude. From this viewpoint, an ideal binary sequence has all nontrivial periodic autocorrelations equal to zero. Such a sequence is called *perfect*. However, the only length  $n > 1$  for which a perfect sequence is known is  $n = 4$ . For example,  $(+ + + -)$  is a perfect sequence (writing  $+$  for 1 and  $-$  for  $-1$ ). In Section 2.3 we shall discuss some results establishing the nonexistence of perfect sequences.

A simple necessary condition for the existence of a perfect binary sequence is contained in the following lemma, which follows from a simple parity argument.

**Lemma 2.1.1.** *All periodic autocorrelations of a binary sequence of length  $n$  are congruent to  $n$  modulo 4.*

Lemma 2.1.1 implies that every binary sequence  $A$  of length  $n > 1$  satisfies

$$(2.1) \quad \max_{0 < u < n} |R_u(A)| \geq \begin{cases} 0 & \text{for } n \equiv 0 \pmod{4} \\ 1 & \text{for } n \equiv 1 \text{ or } 3 \pmod{4} \\ 2 & \text{for } n \equiv 2 \pmod{4} \end{cases}$$

and so perfect binary sequences can exist only when the length is divisible by 4. Indeed since

$$(2.2) \quad \sum_{u=0}^{n-1} R_u(A) = \left| \sum_{k=0}^{n-1} A(k) \right|^2,$$

the length of a perfect binary sequence must be an even square. We call a binary sequence  $A$  *optimal* if equality holds in (2.1). We shall see below that there are infinitely many lengths congruent to 2 or 3 modulo 4 for which optimal binary sequences exist. However, if  $n \equiv 1 \pmod{4}$ , then optimal binary sequences are known only for  $n = 5$  or 13. For example,

$$(2.3) \quad (+ + + - +) \quad \text{and} \quad (+ + + + + - - + + - + - +)$$

are optimal binary sequences of length 5 and 13, respectively. Some nonexistence results will be discussed in Section 2.3.

Sometimes, applications require *balanced* binary sequences, by which we mean binary sequences  $A$  of length  $n$  satisfying

$$\left| \sum_{k=0}^{n-1} A(k) \right| \leq 1.$$

It follows from Lemma 2.1.1 and the identity (2.2) that an optimal binary sequence  $A$  of length  $n$  cannot be balanced if  $n$  is congruent to 0 or 1 modulo 4. Therefore, every balanced binary sequence  $A$  of length  $n > 1$  satisfies

$$(2.4) \quad \max_{0 < u < n} |R_u(A)| \geq \begin{cases} 1 & \text{for } n \equiv 3 \pmod{4} \\ 2 & \text{for } n \equiv 2 \pmod{4} \\ 3 & \text{for } n \equiv 1 \pmod{4} \\ 4 & \text{for } n \equiv 0 \pmod{4}. \end{cases}$$

If  $A$  is a balanced binary sequence of length  $n > 1$  for which equality holds in (2.4), then we say that  $A$  is *optimal balanced*.

We now show that optimal balanced binary sequences exist for infinitely many lengths of every congruence class modulo 4.

**Definition 2.1.2** (Legendre sequences). For an odd prime  $p$ , a *Legendre sequence*  $A$  of length  $p$  is defined by

$$A(k) = \begin{cases} 1 & \text{for } p \mid k \text{ or } k \text{ a square modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

The following result is classical (see [90], for example).

**Theorem 2.1.3.** *Legendre sequences are optimal balanced. In particular, the nontrivial periodic autocorrelations of a Legendre sequence of length  $p$  are equal to  $-1$  if  $p \equiv 3 \pmod{4}$  and are in the set  $\{1, -3\}$  if  $p \equiv 1 \pmod{4}$ .*

Therefore there exist optimal balanced binary sequences for all odd prime lengths. To obtain optimal balanced binary sequences of even length, we require the following definition.

**Definition 2.1.4** (Sidelnikov sequences). Let  $q$  be an odd prime power and let  $\theta$  be a primitive element of  $\mathbb{F}_q$ . Define a sequence  $A$  of length  $q - 1$  by

$$A(k) = \begin{cases} 1 & \text{if } \theta^k + 1 \text{ is zero or a square in } \mathbb{F}_q \\ -1 & \text{otherwise.} \end{cases}$$

It is customary to call the above defined sequences *Sidelnikov sequences*. However, to my knowledge, they were first considered by Turyn [112, p. 208-209] and were later studied independently by Sidelnikov [104] and Lempel, Cohn, and Eastman [62].

**Theorem 2.1.5** ([104], [62]). *Sidelnikov sequences are optimal balanced. In particular, the nontrivial periodic autocorrelations of a Sidelnikov sequence of length  $n$  are in the set  $\{-2, 2\}$  if  $n \equiv 2 \pmod{4}$  and are in the set  $\{0, -4\}$  if  $n \equiv 0 \pmod{4}$ .*

Several other constructions of optimal balanced binary sequences are known, as surveyed in detail by Cai and Ding [16]. The currently known constructions in the case that  $n$  is congruent to 3 modulo 4 will be reviewed in Section 2.2. For now, we consider one more important class of binary sequences, namely the *Galois sequences*, which are also known as *m-sequences*. Recall that the *absolute trace function* on  $\mathbb{F}_{2^m}$  is the mapping  $\text{Tr} : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$  given by

$$\text{Tr}(y) = \sum_{j=0}^{m-1} y^{2^j}.$$

**Definition 2.1.6** (Galois sequences). Let  $\theta$  be a primitive element of  $\mathbb{F}_{2^m}$  and let  $a \in \mathbb{F}_{2^m}$  be nonzero. A *Galois sequence*  $A$  of length  $2^m - 1$  is defined by

$$A(k) = \begin{cases} 1 & \text{for } \text{Tr}(a\theta^k) = 0 \\ -1 & \text{for } \text{Tr}(a\theta^k) = 1. \end{cases}$$

Note that the cyclic shifts of a Galois sequence are also Galois sequences. Galois sequences can be equivalently defined (and efficiently generated) using linear feedback shift registers [40].

The following result is an immediate consequence of elementary properties of the trace function.

**Theorem 2.1.7.** *Galois sequences are optimal balanced. In particular, the nontrivial periodic autocorrelations of a Galois sequence are equal to  $-1$ .*

In fact, Galois sequences have a stronger property than balancedness. If  $A$  is a Galois sequence of length  $2^m - 1$  and  $k$  takes on all values in the set  $\{0, 1, \dots, 2^m - 2\}$ , then the  $m$ -tuples

$$(A(k), A(k+1), \dots, A(k+m-1))$$

range through all  $2^m - 1$  possible binary sequences of length  $m$ , except for the all-ones sequence (see [40] or [41], for example).

## 2.2. CYCLIC DIFFERENCE SETS

In this section we consider binary sequences whose nontrivial periodic autocorrelations are all equal, say to  $\gamma$ . Such sequences are said to possess a *two-level* periodic autocorrelation (with one level being the trivial periodic autocorrelation) and are equivalent to cyclic difference sets.

A *difference set* with parameters  $(n, k, \lambda)$  is a  $k$ -subset  $D$  of a finite group  $G$  of order  $n$  such that every non-identity element  $g$  of  $G$  has exactly  $\lambda$  representations  $g = xy^{-1}$  for  $x, y \in G$  (so that  $k(k-1) = \lambda(n-1)$ ). If  $G$  is a cyclic group, then we say that the difference set is *cyclic*. Note that the complement of a difference set is also a difference set, so we may assume that  $k \leq n/2$ .

Let  $G$  be a cyclic group of order  $n$  and fix a generator  $\omega$  of  $G$ . Given a subset  $D$  of  $G$ , we associate with  $D$  a binary sequence  $A$  of length  $n$  via

$$A(k) = \begin{cases} -1 & \text{for } \omega^k \in D \\ 1 & \text{for } \omega^k \notin D. \end{cases}$$

We call  $A$  the *characteristic sequence* of  $D$  (with respect to  $\omega$ ). The following result is classical and readily verified.

**Proposition 2.2.1.** *Let  $D$  be a subset of a cyclic group. Then the characteristic sequence of  $D$  has two-level periodic autocorrelation if and only if  $D$  is a difference set. Moreover, if  $D$  is a difference set with parameters  $(n, k, \lambda)$ , then the nontrivial periodic autocorrelations of its characteristic sequence equal  $n - 4(k - \lambda)$ .*

In the case  $n \not\equiv 2 \pmod{4}$ , an optimal binary sequence is equivalent to a cyclic difference set with parameters

$$(2.5) \quad \left( n, \frac{n - \sqrt{n}}{2}, \frac{n - 2\sqrt{n}}{4} \right) \quad \text{for } n \equiv 0 \pmod{4},$$

$$(2.6) \quad \left( n, \frac{n - \sqrt{2n-1}}{2}, \frac{n + 1 - 2\sqrt{2n-1}}{4} \right) \quad \text{for } n \equiv 1 \pmod{4},$$

$$(2.7) \quad \left( n, \frac{n-1}{2}, \frac{n-3}{4} \right) \quad \text{for } n \equiv 3 \pmod{4}.$$

As mentioned previously, there are only finitely many known cyclic difference sets with parameters (2.5) or (2.6). All known cyclic difference sets with parameters (2.7) occur when  $n$  is either a prime number, a product of twin primes, or a Mersenne number. Examples are given by Legendre sequences of length  $p$  satisfying  $p \equiv 3 \pmod{4}$  and by Galois sequences, in which cases the sets are called *Paley* and *Singer* difference sets, respectively, since related structures were first studied by Paley [90] and Singer [105]. There are several other constructions of such difference sets, or equivalently optimal binary sequences of length  $n \equiv 3 \pmod{4}$ , which we shall review briefly.

*The twin-prime construction* [14]. Let  $p$  and  $p+2$  be prime numbers and let  $X$  and  $Y$  be Legendre sequences of length  $p$  and  $p+2$ , respectively. The sequence  $A$  of length  $p(p+2)$  given by

$$A(k) = \begin{cases} X(k)Y(k) & \text{for } p \nmid k \text{ and } p+2 \nmid k \\ 1 & \text{for } p \mid k \text{ and } p+2 \nmid k \\ -1 & \text{for } p+2 \mid k \end{cases}$$

is the characteristic sequence of a difference set with parameters (2.7).

*The Hall construction* [45]. Let  $p$  be a prime number of the form  $4x^2 + 27$  for  $x \in \mathbb{Z}$  and let  $\theta$  be a primitive root modulo  $p$ . Let  $C_k$  be the set of numbers  $a \in \mathbb{Z}$  for which the congruence  $x^6 \theta^k \equiv a \pmod{p}$  has a solution  $x \in \mathbb{Z}$ . Let  $D$  be either  $C_0 \cup C_1 \cup C_3$  or  $C_0 \cup C_3 \cup C_5$ , depending on whether 3 is contained in  $C_1$  or  $C_5$ , respectively. (By quadratic and cubic reciprocity laws we always have  $3 \in C_1 \cup C_5$ .) The sequence  $A$  of length  $p$  given by

$$A(k) = \begin{cases} -1 & \text{for } k \in D \\ 1 & \text{otherwise} \end{cases}$$

is the characteristic sequence of a difference set with parameters (2.7), called a *Hall difference set*.

*The Maschietti construction* [72]. Let  $\theta$  be a primitive element of  $\mathbb{F}_{2^m}$  and let  $t$  be an integer coprime to  $2^m - 1$  such that the mapping from  $\mathbb{F}_{2^m}$  to  $\mathbb{F}_{2^m}$ , given by  $x \mapsto x^t + x$ , is 2-to-1. The sequence  $A$  of length  $2^m - 1$  given by

$$A(k) = \begin{cases} -1 & \text{if } y^t + y = \theta^k \text{ has a solution } y \in \mathbb{F}_{2^m} \\ 1 & \text{otherwise} \end{cases}$$

is the characteristic sequence of a difference set with parameters (2.7). This construction was first given by Maschietti [72] by establishing a link to monomial hyperovals in finite projective planes. The above description follows Evans, Hollmann, Krattenthaler, and Xiang [27]. Up to equivalences, the only known choices for  $t$  are  $t = 2^i$  for  $\gcd(i, m) = 1$  (in which case we obtain Galois sequences again),  $t = 6$  for odd  $m$ ,  $t = 3 \cdot 2^{(m+1)/2} + 4$  for odd  $m$ ,  $t = 2^{(m+1)/2} + 2^{(3m+1)/4}$  for  $m \equiv 1 \pmod{4}$ , and  $t = 2^{(m+1)/2} + 2^{(m+1)/4}$  for  $m \equiv 3 \pmod{4}$ .

*The Dillon-Dobbertin construction* [19]. Let  $\theta$  be a primitive element of  $\mathbb{F}_{2^m}$ , let  $t$  be an integer coprime to  $m$  satisfying  $0 < t < m/2$ , and write  $d = 4^t - 2^t + 1$ . The sequence  $A$  of length  $2^m - 1$  given by

$$A(k) = \begin{cases} -1 & \text{if } (y+1)^d + y^d + 1 = \theta^k \text{ has a solution } y \in \mathbb{F}_{2^m} \\ 1 & \text{otherwise} \end{cases}$$

is the characteristic sequence of a difference set with parameters (2.7).

*The No-Chung-Yun construction* [19]. Let  $m$  be an integer that is not divisible by 3, write  $t = (m \pm 1)/3$  depending on the congruence class of  $m$  modulo 3 (so that  $t$  is integral), and write  $d = 4^t - 2^t + 1$ . The sequence  $A$  of length  $2^m - 1$  given by

$$A(k) = \begin{cases} -1 & \text{if } (y+1)^d + y^d = \theta^k \text{ has a solution } y \in \mathbb{F}_{2^m} \\ 1 & \text{otherwise} \end{cases}$$

is the characteristic sequence of a difference set. For even  $m$ , this difference set has parameters (2.7). For odd  $m$ , its complement has parameters (2.7). This construction was given by No, Chung, and Yun [85] and the autocorrelation properties were proved by Dillon and Dobbertin [19].

*The Gordon-Mills-Welch construction* [43]. This construction produces new cyclic difference sets from known ones. Let  $s$  and  $m$  be integers with  $1 < s < m$  and  $s \mid m$ . Let  $D$  be a difference set in  $\mathbb{F}_{2^s}^*$  with parameters  $(2^s - 1, 2^{s-1}, 2^{s-2})$  (so that its complement has parameters (2.7)). Let  $C$  be the set of elements  $c \in \mathbb{F}_{2^m}$  with  $\text{Tr}_{2^m/2^s}(c) = 1$ , where  $\text{Tr}_{2^m/2^s}$  is the *relative trace* from  $\mathbb{F}_{2^m}$  to  $\mathbb{F}_{2^s}$ , given by

$$\text{Tr}_{2^m/2^s}(y) = \sum_{j=0}^{m/s-1} y^{2^{sj}}.$$

Then  $\{cd : c \in C, d \in D\}$  is a difference set in  $\mathbb{F}_{2^m}^*$  with parameters  $(2^m - 1, 2^{m-1}, 2^{m-2})$ .

This construction is a rich source of cyclic difference sets because we do not require any further information about  $D$ . In particular, the construction can be iterated. If  $D$  is a Singer difference set, then the characteristic sequence of the new difference set is sometimes called a *GMW sequence* [102].

### 2.3. NONEXISTENCE RESULTS

We have seen that there are infinite families of optimal binary sequences whose lengths are congruent to either 2 or 3 modulo 4. In this section, we review nonexistence results for optimal binary sequences whose lengths are congruent to either 0 or 1 modulo 4. In these cases the sequences are in one-to-one correspondence with cyclic difference sets. It is customary and convenient to identify the parameters of an  $(n, k, \lambda)$  difference set with the tuple  $(n, k, \lambda, m)$ , where  $m = k - \lambda$ .

Our main focus is on the case  $n \equiv 0 \pmod{4}$ , in which case the difference sets have parameters

$$(4u^2, 2u^2 - u, u^2 - u, u^2)$$

and are called *cyclic Hadamard difference sets*. Some comments on the case  $n \equiv 1 \pmod{4}$  will be given at the end of this section.

There is a well known relationship between perfect binary sequences and Hadamard matrices; a square matrix  $H$  of order  $n$  is a *Hadamard matrix* if all of its entries are

$-1$  or  $1$  and  $HH^T = nI$ , where  $I$  is the  $n \times n$  identity matrix. It is readily verified that the circulant matrix of order  $n$  corresponding to a binary sequence of length  $n$  is a Hadamard matrix if and only if the sequence is perfect. For example, writing  $+$  for  $1$  and  $-$  for  $-1$ , the perfect binary sequence  $(+++ -)$  gives the circulant Hadamard matrix

$$\begin{pmatrix} + & + & + & - \\ - & + & + & + \\ + & - & + & + \\ + & + & - & + \end{pmatrix}.$$

An old conjecture due to Ryser [93, p. 134] asserts that there are no circulant Hadamard matrices of order greater than 4. Equivalently, we have the following.

**Conjecture 2.3.1** ([93]). *There is no perfect binary sequence of length  $n > 4$ .*

This conjecture is still open. However strong partial results are known and the most important methods will be reviewed below. It should be emphasised that most of these methods can be applied to difference sets that are not necessarily cyclic and sometimes even to more general combinatorial objects. However, we will restrict ourselves to the case of cyclic difference sets.

We have seen that the length of a perfect binary sequence must be an even square. Turyn [111, p. 336] proved the much deeper result that the length must actually be 4 times an odd square.

**Theorem 2.3.2** ([111]). *If there exists a perfect binary sequence of length  $n \geq 4$ , then  $n = 4u^2$  for an odd integer  $u$ .*

We proceed with a classical result due to Turyn [111], for which we require the following definition. For integers  $a$  and  $w > 0$ , we say that  $a$  is *semiprimitive* modulo  $w$  if there exists an integer  $t$  such that  $a^t \equiv -1 \pmod{w}$  and we say that  $a$  is *self-conjugate* modulo  $w$  if each prime divisor  $p$  of  $a$  is semiprimitive modulo  $w_p$ , where  $w_p$  is the largest divisor of  $w$  that is not divisible by  $p$ .

The following result is [111, Corollary 1] specialised to cyclic difference sets.

**Theorem 2.3.3** ([111]). *Suppose that there exists a cyclic difference set with parameters  $(n, k, \lambda, m)$ . Suppose further that there are positive integers  $c$  and  $d$  satisfying  $\gcd(c, d) > 1$  such that  $d \mid n$  and  $c^2 \mid m$  and such that  $c$  is self-conjugate modulo  $d$ . Let  $r$  be the number of distinct prime divisors of  $\gcd(c, d)$ . Then  $cd \leq 2^{r-1}n$ .*

For convenience, we state Theorem 2.3.3 for perfect binary sequences.

**Corollary 2.3.4.** *Suppose that there exists a perfect binary sequence of length  $n = 4u^2$ . Suppose further that there are positive integers  $c$  and  $d$  satisfying  $\gcd(c, d) > 1$  such that  $d \mid n$  and  $c \mid u$  and such that  $c$  is self-conjugate modulo  $d$ . Let  $r$  be the number of distinct prime divisors of  $\gcd(c, d)$ . Then  $cd \leq 2^{r-1}n$ .*

Corollary 2.3.4 is particularly useful if  $u$  has a relatively large odd prime factor. Indeed, if  $p$  is an odd prime such that  $u = p^a v$  for positive integers  $a$  and  $v$ , then take  $c = p^a$  and  $d = 2p^{2a}$  in Corollary 2.3.4 to conclude that no perfect binary sequence of length  $4u^2$  exists if  $p^a > 2v^2$ . In particular, taking  $v = 1$ , we see that there is no perfect binary sequence whose length is four times an odd prime power.



Corollary 2.3.4 proves the nonexistence of perfect binary sequences of length  $4u^2$  for all  $u$  satisfying  $1 < u < 55$ , except for  $u = 39$ . However, this last case was also ruled out by Turyn [112, p. 202].

It took more than thirty years until the next open case  $u = 55$  was disqualified by B. Schmidt [95], [96] with the invention of a powerful method, known as the “Field Descent Method”. This method was subsequently refined by Leung and B. Schmidt [64], [65]. The results involve a rather technical function  $F(n, m)$ , which we define below (our definition is taken from [64] and is equivalent to the original definition of [95] modulo a slight inaccuracy). Recall the following standard notation. For integers  $a$  and  $w > 0$ , the number  $\text{ord}_w(a)$  is the smallest positive integer  $t$  such that  $a^t \equiv 1 \pmod{w}$ . For positive integers  $r$  and  $b$ , the number  $\nu_r(b)$  is the largest integer  $t$  such that  $r^t$  divides  $b$ .

**Definition 2.3.5.** For an integer  $k$ , denote by  $\mathfrak{D}(k)$  the set of prime divisors of  $k$ . Let  $n$  and  $m$  be integers greater than 1. For  $q \in \mathfrak{D}(m)$ , write

$$n(q) = \begin{cases} \prod_{p \in \mathfrak{D}(n) \setminus \{q\}} p & \text{if } n \text{ is odd or } q = 2, \\ 4 \prod_{p \in \mathfrak{D}(n) \setminus \{2, q\}} p & \text{otherwise.} \end{cases}$$

Put

$$b(r, n, m) = \begin{cases} \max_{q \in \mathfrak{D}(m) \setminus \{2\}} \{ \nu_2(q^2 - 1) + \nu_2(\text{ord}_{n(q)}(q)) - 1 \} & \text{for } r = 2, \\ \max_{q \in \mathfrak{D}(m) \setminus \{r\}} \{ \nu_r(q^{r-1} - 1) + \nu_r(\text{ord}_{n(q)}(q)) \} & \text{for } r > 2 \end{cases}$$

with the convention that  $b(2, n, m) = 2$  if  $\mathfrak{D}(m) = \{2\}$  and  $b(r, n, m) = 1$  if  $\mathfrak{D}(m) = \{r\}$  and  $r > 2$ . We define

$$F(n, m) = \gcd \left( n, \prod_{p \in \mathfrak{D}(n)} p^{b(p, n, m)} \right).$$

Elementary number theory implies the useful fact that, if  $n$  and  $m$  are integers greater than 1, then every prime divisor of  $n$  is also a divisor of  $F(n, m)$ .

The following result is the cyclic group case of [64, Theorem 4.3], which generalises [95, Theorem 5.3]. We denote by  $\phi(n)$  Euler’s totient function.

**Theorem 2.3.6** ([64]). *Let  $G = A \times H$  be a cyclic group such that  $\gcd(|A|, |H|) = 1$ . If  $G$  contains an  $(n, k, \lambda, m)$  difference set with  $\gcd(m, |H|) = 1$ , then*

$$m \leq \frac{|H|F^2}{4\phi(F)},$$

where  $F = \gcd(|A|, F(n, m))$ .

In the case of cyclic Hadamard difference sets, we have  $n = 4u^2$  for  $u$  odd by Theorem 2.3.2, so that we can always take  $|H| = 4$  in Theorem 2.3.6. It can be shown that this is always a better choice than  $|H| = 1$ . Application of Theorem 2.3.6 with  $|H| = 4$  to cyclic Hadamard difference sets gives the following result (see [64, Corollary 4.5]).

**Corollary 2.3.7** ([64]). *If there exists a perfect binary sequence of length  $4u^2$ , then  $u\phi(u) \leq F(u^2, u)$ .*

A combination of Corollaries 2.3.4 and 2.3.7 implies that there is no perfect binary sequence of length  $4u^2$  for  $1 < u < 11\,715$  [64, Corollary 4.5]. Hence we have the following result.

**Corollary 2.3.8** ([64]). *There is no perfect binary sequence of length  $n$  for  $4 < n < 548\,964\,900$ .*

We illustrate the application of Corollary 2.3.7 for perfect binary sequences of length 12 100, which is the first case where Turyn's results [111] are insufficient to prove nonexistence.

**Example 2.3.9.** Take  $n = 4u^2$  for  $u = 55$ , so that  $n = 12\,100$ . To apply Corollary 2.3.7, we require the value of  $F(55^2, 55)$ . We have  $\text{ord}_{n(5)}(5) = \text{ord}_{11}(5) = 5$  and  $\text{ord}_{n(11)}(11) = \text{ord}_5(11) = 1$  and therefore

$$\begin{aligned} b(5, 55^2, 55) &= \nu_5(11^4 - 1) + \nu_5(1) = 1 \\ b(11, 55^2, 55) &= \nu_{11}(5^{10} - 1) + \nu_{11}(5) = 1, \end{aligned}$$

from which we conclude that

$$F(55^2, 55) = \gcd(55^2, 5^1 \cdot 11^1) = 55.$$

Since  $\phi(55) = 40$ , by Corollary 2.3.7 the existence of a perfect binary sequence of length 12 100 implies  $55 \cdot 40 \leq 55$ , a contradiction. Therefore there is no perfect binary sequence of length 12 100.

Mossinghoff [78], Borwein and Mossinghoff [12], and Logan and Mossinghoff [71] proposed clever methods in order to identify numbers  $n$  for which Corollary 2.3.7 does not prove nonexistence of a perfect binary sequence of length  $n$ . For many of these numbers, nonexistence follows from Corollary 2.3.4 or some further nonexistence results by Leung and Schmidt [65], which also involve self-conjugacy arguments and the field descent method. Most notably, Leung and Schmidt [66] recently developed a new method, which they call the “Anti-Field-Descent Method”, which provides further strong, albeit rather technical, nonexistence results. However, the smallest length for which the existence of a perfect binary sequences has not been decided so far is still 548 964 900.

We close this section with some comments on optimal binary sequences of length  $n$  for  $n \equiv 1 \pmod{4}$ . Such sequences are in one-to-one correspondence with cyclic difference sets having parameters

$$(2.8) \quad (2u^2 + 2u + 1, u^2, \tfrac{1}{2}u(u-1), \tfrac{1}{2}u(u+1))$$

for a positive integer  $u$ . The cases  $u = 1$  and  $u = 2$  correspond to the binary sequences (2.3). Turyn [112, p. 199] reports nonexistence of these difference sets for  $3 \leq u \leq 11$ . Eliahou and Kervaire [23] used the following result due to Lander [61, Theorem 4.5] to obtain further nonexistence results.

**Theorem 2.3.10** ([61]). *Suppose that there exists a cyclic difference set with parameters  $(n, k, \lambda, m)$ . Let  $d$  be a divisor of  $n$  with  $d > 1$  and let  $p$  be a prime. If  $p$  is semiprimitive modulo  $d$ , then  $p$  does not divide the square-free part of  $m$ . Moreover, if  $d = n$ , then  $p$  does not divide  $n$  itself.*

Theorem 2.3.10 implies the nonexistence of cyclic difference sets with parameters (2.8) for all  $u$  satisfying  $3 \leq u \leq 100$ , except for  $u \in \{9, 49, 50, 82\}$  (see [23, Table I] for

details). The latter four cases can be ruled out [23], [15] using multiplier theory. Hence there is no optimal binary sequence of length  $n$  for  $n \equiv 1 \pmod{4}$  and  $13 < n < 20605$ .

Of course these results suggest a conjecture, which, to my knowledge, has not been stated explicitly in the literature.

**Conjecture 2.3.11.** *There is no optimal binary sequence of length  $n > 13$  for  $n \equiv 1 \pmod{4}$ . Equivalently there is no cyclic difference set with parameters (2.8) for  $u > 2$ .*

### 3. APERIODIC AUTOCORRELATION OF BINARY SEQUENCES

#### 3.1. BARKER SEQUENCES

For every binary sequence  $A$  of length  $n$ , the aperiodic autocorrelation  $C_u(A)$  is an integer with parity  $n-u$ . A *Barker sequence* is a binary sequence with the ideal property that all nontrivial aperiodic autocorrelations are either 0 or 1 in magnitude. (Barker's original definition [5] requires that all nontrivial aperiodic autocorrelations are either 0 or  $-1$ , but it has become customary to impose our slightly less restrictive condition.)

Notice that for fixed  $a, b \in \{0, 1\}$ , the transformation  $A(k) \mapsto A(k)(-1)^{a+bk}$  preserves the Barker property. We can therefore assume without loss of generality that a Barker sequence  $A$  satisfies  $A(1) = A(2) = 1$ . The only known Barker sequences with this property are (writing  $+$  for 1 and  $-$  for  $-1$ )

$$\begin{aligned} n = 2 : & \quad (++) , \\ n = 3 : & \quad (++) , \\ n = 4 : & \quad (+++-), \quad (++-+), \\ n = 5 : & \quad (++++-), \\ n = 7 : & \quad (++++--+-), \\ n = 11 : & \quad (++++--+-+--), \\ n = 13 : & \quad (+++++--++--+-). \end{aligned}$$

Indeed, it has been conjectured since at least 1960 [107] that there are no other lengths for which Barker sequences exist.

**Conjecture 3.1.1** ([107]). *There is no Barker sequence of length greater than 13.*

This conjecture is known to be true for sequences of odd length, as proven by Turyn and Storer [110]. A simpler proof was recently given by Schmidt and Willms [101].

**Theorem 3.1.2** ([110], [101]). *There is no Barker sequence of odd length greater than 13.*

Indeed, the case that the length is odd in Conjecture 3.1.1 appears to be considerably easier than the case of even length for the following reason. Since exactly one of  $u$  or  $n-u$  is odd for odd  $n$ , it follows from (1.1) and Lemma 2.1.1 that a Barker sequence  $A$  of odd length  $n$  satisfies

$$C_u(A) = \begin{cases} 0 & \text{for even } u > 0 \\ (-1)^{(n-1)/2} & \text{for odd } u. \end{cases}$$

This fixes all aperiodic autocorrelations of a Barker sequence of odd length, which is the key to prove Theorem 3.1.2. A similar reasoning implies that a Barker sequence

of even length greater than 2 must have length a multiple of 4 and all of its nontrivial periodic autocorrelations equal to zero. Hence we have the following.

**Proposition 3.1.3.** *Every Barker sequence of even length greater than 2 is a perfect binary sequence.*

In view of Proposition 3.1.3 and Theorem 3.1.2, Turyn's Conjecture 3.1.1 is implied by Ryser's Conjecture 2.3.1 and all nonexistence results for perfect binary sequences immediately provide nonexistence results for Barker sequences. In particular, by Theorem 2.3.2, the length of a Barker sequence of even length greater than 2 is four times an odd square and, by Corollary 2.3.8, there is no Barker sequence of even length  $n$  for  $4 < n < 548\,964\,900$ . The only known nonexistence result for Barker sequences of even length that is not implied by results for perfect binary sequences is the following result due to Eliahou, Kervaire, and Saffari [25] (which as explained in [25] follows from the forthcoming Proposition 5.2.6).

**Theorem 3.1.4** ([25]). *If a Barker sequence of even length  $n$  exists, then every odd prime divisor of  $n$  is congruent to 3 modulo 4.*

As shown by Mossinghoff [78], the combination of Corollaries 2.3.4 and 2.3.7 and Theorem 3.1.4 implies that there is no Barker sequence of even length  $n$  for

$$4 < n < 189\,260\,468\,001\,034\,441\,522\,766\,781\,604.$$

Refined methods by Borwein and Mossinghoff [12] and Leung and Schmidt [65], [66] imply the following slightly stronger result.

**Proposition 3.1.5.** *There is no Barker sequence of even length  $n$  for  $4 < n \leq 4 \cdot 10^{33}$ .*

As noted by Leung and Schmidt [66], there are currently 8125 known numbers  $n$  up to  $10^{100}$  for which the known methods fail to settle the nonexistence of a Barker sequence of length  $n$ . The smallest of these numbers is larger than  $10^{51}$ , namely  $4u^2$  for  $u = 30109 \cdot 1128713 \cdot 2167849 \cdot 268813277$ . However it is not clear whether these known open cases are exhaustive for  $n \leq 10^{100}$ .

### 3.2. MEASURES OF SMALLNESS OF APERIODIC AUTOCORRELATIONS

In response to the presumed nonexistence of long Barker sequences, several authors have studied different measures for the collective smallness of the aperiodic autocorrelations of sequences. For a sequence  $A$  of length  $n$  and a real number  $r > 0$ , define

$$M_r(A) = \left( \sum_{0 < u < n} |C_u(A)|^r \right)^{1/r}$$

and

$$M(A) = \max_{0 < u < n} |C_u(A)|,$$

which equals the limit of  $M_r(A)$  as  $r \rightarrow \infty$ . We are interested in minimising these functions over the set of binary sequences of a given length. Accordingly, we define the arithmetic functions

$$(3.1) \quad m_r(n) = \min_{A \in \mathfrak{B}_n} M_r(A)$$

and

$$(3.2) \quad m(n) = \min_{A \in \mathfrak{B}_n} M(A),$$

where  $\mathfrak{B}_n$  is the set of binary sequences of length  $n$ . The principal problem is to understand the behaviour of these functions as  $n$  tends to infinity.

Two measures have received particular attention:  $M(A)$ , called the *peak sidelobe level* of  $A$ , and  $M_2(A)$ , which is essentially the sum of squares of the nontrivial aperiodic autocorrelations of  $A$ .

In Section 3.3, we shall see how probabilistic methods help to understand the asymptotic behaviour of the functions  $m(n)$  and  $m_r(n)$ . In Sections 3.4 and 3.5, we study the measures  $M(A)$  and  $M_2(A)$ , respectively, where our focus is in particular on constructive results.

### 3.3. RANDOM BINARY SEQUENCES

In this section our goal is to obtain information on the growth rate of the functions  $m(n)$  and  $m_r(n)$  using probabilistic methods. As before,  $\mathfrak{B}_n$  denotes the set of binary sequences of length  $n$  and, throughout this section,  $A_n$  is drawn at random from  $\mathfrak{B}_n$ , equipped with the uniform probability measure. In other words, each of the  $n$  entries in  $A_n$  is drawn independently from  $\{-1, 1\}$  with  $\Pr(-1) = \Pr(1) = 1/2$ . By  $E(X)$  we denote the expectation of a random variable  $X$ .

We are interested in the asymptotic behaviour, as  $n \rightarrow \infty$ , of  $M(A)$  and  $M_r(A)$  for most binary sequences  $A$  of length  $n$ . This problem was first studied by Moon and Moser [77] for the peak sidelobe level  $M(A)$ . In particular, they asked for arithmetic functions  $L(n)$  and  $U(n)$  such that

$$\lim_{n \rightarrow \infty} \Pr \left[ L(n) \leq M(A_n) \leq U(n) \right] = 1.$$

This implies in particular that  $m(n)$  grows not faster than  $U(n)$ .

Some nontrivial results for such functions  $L(n)$  and  $U(n)$  were given by Moon and Moser [77], which were later improved by Mercer [75] and Alon, Litsyn, and Shpant [1]. Further improvements by the author [100] show that we can in fact take

$$L(n) = (1 - \epsilon)\sqrt{2n \log n} \quad \text{and} \quad U(n) = (1 + \epsilon)\sqrt{2n \log n}$$

for an arbitrary  $\epsilon > 0$ . To state the result slightly more formally, recall that a sequence of random variables  $X_1, X_2, \dots$  *converges in probability* to a constant  $c$  if

$$\Pr[|X_n - c| > \epsilon] \rightarrow 0$$

as  $n \rightarrow \infty$  for all  $\epsilon > 0$ .

**Theorem 3.3.1** ([100]). *Let  $A_n$  be drawn at random from  $\mathfrak{B}_n$ , equipped with the uniform probability measure. Then, as  $n \rightarrow \infty$ ,*

$$\frac{M(A_n)}{\sqrt{n \log n}} \rightarrow \sqrt{2} \quad \text{in probability}$$

and

$$\frac{E(M(A_n))}{\sqrt{n \log n}} \rightarrow \sqrt{2}.$$

In [98], the following complementary result for  $M_r(A_n)$  was proved, in which  $\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt$  denotes the *gamma function*, satisfying  $\Gamma(p+1) = p!$  when  $p$  is a nonnegative integer.

**Theorem 3.3.2.** [98] *Let  $A_n$  be drawn at random from  $\mathfrak{B}_n$ , equipped with the uniform probability measure, and let  $r$  be a positive real number. Then, as  $n \rightarrow \infty$ ,*

$$\frac{M_r(A_n)}{n^{1/2+1/r}} \rightarrow \left( \frac{\Gamma(r+1)}{2^{r/2} \Gamma(r/2+2)} \right)^{1/r} \quad \text{in probability}$$

and

$$(3.3) \quad \frac{\mathbb{E}(M_r(A_n)^r)}{n^{r/2+1}} \rightarrow \frac{\Gamma(r+1)}{2^{r/2} \Gamma(r/2+2)}.$$

Moreover, for  $r \geq 1$ , as  $n \rightarrow \infty$ ,

$$\frac{\mathbb{E}(M_r(A_n))}{n^{1/2+1/r}} \rightarrow \left( \frac{\Gamma(r+1)}{2^{r/2} \Gamma(r/2+2)} \right)^{1/r}.$$

Theorems 3.3.1 and 3.3.2 provide upper bounds for the growth rate of the functions  $m(n)$  and  $m_r(n)$ , namely

$$(3.4) \quad \limsup_{n \rightarrow \infty} \frac{m(n)}{\sqrt{n \log n}} \leq \sqrt{2}$$

and

$$(3.5) \quad \limsup_{n \rightarrow \infty} \frac{m_r(n)}{n^{1/2+1/r}} \leq \left( \frac{\Gamma(r+1)}{2^{r/2} \Gamma(r/2+2)} \right)^{1/r}.$$

In Section 3.4, we provide an explicit construction, which shows that (3.4) can be improved to

$$m(n) \leq \sqrt{2n \log(2n)} \quad \text{for all } n > 1.$$

For finite  $r \neq 2$ , nothing stronger than (3.5) is known, and for  $r = 2$ , the best known result is

$$\limsup_{n \rightarrow \infty} m_2(n)/n \leq c,$$

where  $c < 25/89$  is strictly smaller than  $1/\sqrt{2}$  (see the forthcoming Corollary 3.5.6).

When  $r$  is a positive integer, the exact values of  $\mathbb{E}(M_r(A_n)^r)$  are known. Since a random variable cannot always exceed its expected value, such values give bounds for  $m_r(n)$  for integral  $r$  and specific values of  $n$ . Mercer [75] showed that, when  $r$  is an even positive integer, then  $\mathbb{E}(M_r(A_n)^r)$  is a polynomial of degree  $r/2 + 1$  in  $n$ . By (3.3), the leading coefficient of this polynomial is

$$\frac{r!}{2^{r/2} (r/2 + 1)!}.$$

For example,

$$(3.6) \quad \begin{aligned} \mathbb{E}(M_2(A_n)^2) &= \frac{1}{2}(n^2 - n), \\ \mathbb{E}(M_4(A_n)^4) &= \frac{1}{2}(2n^3 - 5n^2 + 3n). \end{aligned}$$

The author showed [98] that, when  $r$  is an odd positive integer, then

$$\frac{4^n}{\binom{2n}{n}} \mathbb{E}(M_r(A_{2n})^r) \quad \text{and} \quad \frac{4^n}{\binom{2n}{n}} \mathbb{E}(M_r(A_{2n+1})^r)$$

are polynomials of degree  $(r+3)/2$  in  $n$ . It can be deduced from (3.3) that the leading term of these polynomials is

$$\frac{2^{r+2} \left(\frac{r-1}{2}\right)!}{r+2}.$$

For example,

$$\begin{aligned} E(M_1(A_{2n})) &= \binom{2n}{n} \frac{8n^2 - 2n}{3 \cdot 4^n}, \\ E(M_1(A_{2n+1})) &= \binom{2n}{n} \frac{8n^2 + 4n}{3 \cdot 4^n}, \\ E(M_3(A_{2n})^3) &= \binom{2n}{n} \frac{96n^3 - 68n^2 + 2n}{15 \cdot 4^n}, \\ E(M_3(A_{2n+1})^3) &= \binom{2n}{n} \frac{96n^3 + 52n^2 + 2n}{15 \cdot 4^n}. \end{aligned}$$

### 3.4. THE PEAK SIDELobe LEVEL OF BINARY SEQUENCES

In this section we continue to study the function  $m(n)$ , defined in (3.2). We are in particular interested in constructive existence results. The value of  $m(n)$  has been determined via exhaustive search for all  $n \leq 80$  (see [63] for the latest results). Many authors have put considerable computational effort in finding binary sequences with small peak sidelobe level (see Nunn and Coxson [87], for example), showing that the function  $m(n)$  satisfies

$$\begin{aligned} (3.7) \quad m(n) &\leq 1 \quad \text{for each } n \leq 5, \\ m(n) &\leq 2 \quad \text{for each } n \leq 21, \\ m(n) &\leq 3 \quad \text{for each } n \leq 48, \\ m(n) &\leq 4 \quad \text{for each } n \leq 82, \\ m(n) &\leq 5 \quad \text{for each } n \leq 105. \end{aligned}$$

Turyn conjectured [108], [112, p. 198] that the infimum limit of  $m(n)$  is infinite. Ein-Dor, Kanter, and Kinzel [22] used a heuristic argument to obtain an “educated guess” about the growth of the function  $m(n)$ . We summarise their results in the following form.

**Conjecture 3.4.1.** *As  $n \rightarrow \infty$ , we have*

$$\frac{m(n)}{\sqrt{n}} \rightarrow d, \quad \text{where } d = 0.435 \dots$$

If  $A_n$  is drawn from the set of binary sequences of length  $n$ , equipped with the uniform probability measure, then there are dependencies among the random variables

$$(3.8) \quad \frac{C_1(A_n)}{\sqrt{n-1}}, \frac{C_2(A_n)}{\sqrt{n-2}}, \dots, \frac{C_{n-1}(A_n)}{\sqrt{1}}.$$

The underlying heuristic assumption leading to the conclusion of Conjecture 3.4.1 is to treat (3.8) as mutually independent standard normal random variables. The normality is partly justified by the central limit theorem. The independence is also partly justified:

The methods used to prove [98, Proposition 7] can be used to show that, for a *fixed* positive integer  $v$ , the random vector

$$\left( \frac{C_1(A_n)}{\sqrt{n-1}}, \frac{C_2(A_n)}{\sqrt{n-2}}, \dots, \frac{C_v(A_n)}{\sqrt{n-v}} \right)$$

converges in distribution to a multivariate normal distribution with identity covariance matrix. The known values of  $m(n)$  also lend evidence in favour of Conjecture 3.4.1. Writing  $f(x) = 0.435\sqrt{x}$ , then  $f(x) - 1$  changes sign for  $x \in (5, 6)$ ,  $f(x) - 2$  changes sign for  $x \in (21, 22)$ , and  $f(x) - 3$  changes sign for  $x \in (47, 48)$ . This should be compared with the data in (3.7).

In the remainder of this section, we discuss constructive results. In [97] the author gives a construction for a binary sequence of length  $n$  with peak sidelobe level at most  $\sqrt{2n \log(2n)}$  for every  $n > 1$ , thus showing that

$$m(n) \leq \sqrt{2n \log(2n)}.$$

The construction is inspired by a method in probabilistic combinatorics, known as derandomisation.

**Construction 3.4.2** ([97]). *Let  $n$  be a positive integer and construct a binary sequence  $B_n$  of length  $n$  recursively by*

$$B_n(k) = -\text{sign} \left[ \sum_{u=1}^{k-1} B_n(k-u) \sinh \left( \sqrt{\frac{2 \log(2n)}{n}} \sum_{j=0}^{k-u-1} B_n(j) B_n(j+u) \right) \right],$$

where, by convention,  $\text{sign}(0) = -1$ .

As shown in [97], the sequence  $B_n$  can be efficiently constructed with  $O(n^2)$  multiplications and additions.

**Theorem 3.4.3** ([97]). *The binary sequence  $B_n$  of length  $n > 1$  obtained under Construction 3.4.2 satisfies  $M(B_n) \leq \sqrt{2n \log(2n)}$ .*

Theorem 3.4.3 gives the currently best known upper bound for infinitely many values of  $m(n)$ , although it guarantees only a peak sidelobe level of roughly the same as that of a typical binary sequence (see Theorem 3.3.1). Numerical results [97] however lend evidence to the following conjecture.

**Conjecture 3.4.4** ([97]). *Let  $B_n$  be the binary sequence of length  $n$  obtained under Construction 3.4.2. Then there exist positive constants  $c_1$  and  $c_2$  such that, for all  $n > 1$ ,*

$$c_1 \sqrt{n \log \log n} \leq M(B_n) \leq c_2 \sqrt{n \log \log n}.$$

Some examples for small  $n$  reveal that, if  $c_2$  in Conjecture 3.4.4 exists, then  $c_2$  must be strictly greater than 1. It is however conceivable that

$$\limsup_{n \rightarrow \infty} \frac{M(B_n)}{\sqrt{n \log \log n}} \leq 1.$$

The correctness of Conjecture 3.4.4 implies that the sequences  $B_n$  are exceptional in the sense that their peak sidelobe level grows strictly more slowly than that of most binary sequences, as given in Theorem 3.3.1.

Further candidates of families of binary sequences whose peak sidelobe grows more slowly than that of most binary sequences are Legendre sequences and Galois sequences



(see Section 2.1), although the currently known proven results are not as strong as those in Theorem 3.4.3.

A *cyclic shift* by  $r$  elements of a sequence  $A$  of length  $n$  is the sequence of length  $n$  whose  $k$ -th entry is  $A(k+r)$ , where as usual the index is reduced modulo  $n$ . Note that, while the periodic autocorrelations remain unchanged for all cyclic shifts of a sequence, the aperiodic autocorrelations can vary considerably over the cyclic shifts of a sequence.

For Legendre sequences, the following result was proved by Mauduit and Sárközy [73].

**Theorem 3.4.5** ([73]). *The peak sidelobe level of every cyclic shift of a Legendre sequence of (prime) length  $p$  is at most  $1 + 18\sqrt{p} \log p$ .*

Numerical investigations by Boehmer [8], Turyn [112, p. 203], and in particular by Jedwab and Yoshida [57] suggest that the bound of Theorem 3.4.5 can be improved, perhaps to a small constant times  $\sqrt{p \log p}$ .

For Galois sequences, the following result was proved by Sarwate [94].

**Theorem 3.4.6** ([94]). *The peak sidelobe level of a Galois sequence of length  $n = 2^m - 1$  is at most  $1 + (2/\pi)\sqrt{n+1} \log(4n/\pi)$ .*

Note that every cyclic shift of a Galois sequence is also a Galois sequence, so Theorem 3.4.6 also applies to all cyclic shifts of a Galois sequence.

We shall see in Theorem 3.5.7 that the asymptotic behaviour of  $M_2(A)$  is known for Galois sequences. A combination with the standard norm inequality

$$M(A) n^{1/2} \geq M_2(A),$$

valid for arbitrary sequences  $A$  of length  $n > 1$ , implies the following asymptotic lower bound.

**Theorem 3.4.7.** *Let  $n$  take values only in the set of Mersenne numbers and let  $Y_n$  be a Galois sequence of length  $n$ . Then*

$$\liminf_{n \rightarrow \infty} \frac{M(Y_n)}{n^{1/2}} \geq \frac{1}{\sqrt{6}}.$$

A similar result can also be established for Legendre sequences. Theorems 3.4.6 and 3.4.7 determine the asymptotic behaviour of the peak sidelobe level of Galois sequences up to a factor of roughly  $\log n$ . Numerical results suggest that the upper bound in Theorem 3.4.6 can be improved. In particular, extensive numerical investigations by Dmitriev and Jedwab [21] give evidence supporting the following conjecture.

**Conjecture 3.4.8.** *The peak sidelobe level of a Galois sequence of length  $n = 2^m - 1$  is at most  $C\sqrt{n} \log \log n$  for some absolute constant  $C$ .*

The correctness of Conjecture 3.4.8 implies that Galois sequences are exceptional in the sense that their peak sidelobe level grows strictly more slowly than that of most binary sequences.

Even more striking observations can be obtained from a numerical analysis of random Galois sequences. It is well known that there are exactly  $n\phi(n)/m$  Galois sequences of length  $n = 2^m - 1$ , where  $\phi(n)$  is Euler's totient function. Numerical investigations by Dmitriev and Jedwab [21] lend strong evidence to the following conjecture.

**Conjecture 3.4.9.** *Let  $n$  take values only in the set of Mersenne numbers. Let  $Y_n$  be drawn from the set of Galois sequences of length  $n$ , equipped with the uniform probability measure, and let  $W(Y_n)$  be the maximum peak sidelobe level over all cyclic shifts of  $Y_n$ . Then the limit*

$$\lim_{n \rightarrow \infty} \frac{E(W(Y_n))}{\sqrt{n}}$$

*exists and is finite.*

Indeed it has been verified in [21] that, with the notation as in Conjecture 3.4.9, the value  $E(W(Y_n))/\sqrt{n}$  lies within 3% of 1.31 for all values of  $m$  between 13 and 25. The correctness of Conjectures 3.4.1 and 3.4.9 would imply that the family of Galois sequences contains a subfamily whose peak sidelobe level is nearly optimal.

### 3.5. THE MERIT FACTOR OF BINARY SEQUENCES

In this section we are interested in the measure  $M_2(A)$  for binary sequences  $A$ , or equivalently, in the sum of squares of the nontrivial aperiodic autocorrelations of binary sequences. For a sequence  $A$  of length  $n$ , it is customary to study the normalised measure

$$F(A) = \frac{C_0(A)^2}{2 \sum_{0 < u < n} |C_u(A)|^2}$$

(provided that the denominator is nonzero), which Golay [38] called the *merit factor* of  $A$ . A large merit factor means that the sum of squares of the nontrivial autocorrelations is small when compared to the squared trivial autocorrelation (which always equals  $n^2$  for binary sequences of length  $n$ ).

The determination of the largest possible merit factor of long binary sequences is of considerable importance in various contexts. In digital communications, binary sequences with large merit factor correspond to signals whose energy is very uniformly distributed over frequency [6]. In theoretical physics, binary sequences achieving the largest merit factor for their length correspond to the ground states of Bernasconi's Ising spin model [7]. The growth rate of the optimal merit factor of binary sequences, as the sequence length increases, is related to classical conjectures due to Littlewood [69], [70] and Erdős [26], [84] on the asymptotic behaviour of norms of polynomials on the unit circle.

This latter relationship arises because, when a sequence  $A$  of length  $n$  is represented as a polynomial  $f_A(z) = \sum_{k=0}^{n-1} A(k)z^k$ , its merit factor  $F(A)$  satisfies

$$F(A) = \frac{\|f_A\|_2^4}{\|f_A\|_4^4 - \|f_A\|_2^4},$$

where, for  $1 \leq \alpha < \infty$ ,

$$\|f_A\|_\alpha = \left( \frac{1}{2\pi} \int_0^{2\pi} |f_A(e^{i\phi})|^\alpha d\phi \right)^{1/\alpha}$$

is the  $L^\alpha$  norm on the unit circle of the polynomial  $f_A(z)$ . Note that  $\|f_A\|_2 = \sqrt{n}$  if  $A$  is a unimodular sequence of length  $n$ . There is an extensive body of research dealing with extremal problems for such norms (see [9] for a survey of selected problems).

Define

$$\varphi(n) = \max_{A \in \mathfrak{B}_n} F(A),$$

where  $\mathfrak{B}_n$  is the set of binary sequences of length  $n$ . This function is related to the function  $m_2(n)$ , defined in (3.1), via  $2\varphi(n) = (n/m_2(n))^2$ . It follows from (3.6) that, when  $A$  is drawn uniformly at random from  $\mathfrak{B}_n$ , then  $E(1/F(A)) = 1 - 1/n$ , which gives a lower bound for  $\varphi(n)$ . Various conjectures on the asymptotic behaviour of  $\varphi(n)$  have appeared in the literature. We mention in particular two contradicting conjectures by Golay [39] and Littlewood [69].

**Conjecture 3.5.1** ([39]).  $\lim_{n \rightarrow \infty} \varphi(n)$  exists and equals 12.32...

**Conjecture 3.5.2** ([69]).  $\limsup_{n \rightarrow \infty} \varphi(n) = \infty$ .

Conjecture 3.5.1 uses the same heuristic reasoning as that leading to Conjecture 3.4.1 for the minimum peak sidelobe level. Apparently, Conjecture 3.5.2 is based solely on (very limited) numerical data.

In view of the above conjectures, it is interesting that Fredman, Saffari, and Smith [34] proved that symmetric binary sequences have bounded merit factor. In particular, [34] contains the following more precise result.

**Theorem 3.5.3** ([34]). *Let  $A$  be a unimodular sequence of length  $n$  satisfying  $A(n - 1 - k) = \overline{A(k)}$  for  $0 \leq k < n$ . Then*

$$\frac{1}{F(A)} \geq \sup_{\lambda > 0} \frac{1}{\cosh(2\lambda)} \left( \frac{(\sinh \lambda)^2}{\lambda^2} - 1 \right).$$

*In particular,  $F(A) < 9.55$ .*

The strongest existence result that Littlewood was able to prove [70] arises from a construction due to Shapiro [103], [92]. Take  $A_0 = B_0 = (1)$  and construct binary sequences  $A_m$  and  $B_m$  of length  $2^m$  recursively with the rule

$$(3.9) \quad A_{m+1} = (A_m, B_m) \quad \text{and} \quad B_{m+1} = (A_m, -B_m).$$

The sequences  $A_m$  and  $B_m$  are called the *Shapiro sequences* of length  $2^m$ .

**Theorem 3.5.4** ([70]). *Let  $A_m$  be either Shapiro sequence of length  $2^m$ . Then*

$$F(A_m) = \frac{3}{1 - (-1/2)^m}.$$

*In particular, the asymptotic merit factor as  $m \rightarrow \infty$  of Shapiro sequences equals 3.*

Theorem 3.5.4 was first proved by Littlewood [70, Chapter III, Problem 19], but was later obtained independently by Høholdt, Jensen, and Justesen [50] and Newman and Byrnes [84]. Merit factors of generalisations of Shapiro sequences have also been studied in [50] and [11].

The result of Theorem 3.5.4 was subsequently improved by Høholdt and Jensen [49] and by Jedwab, Katz, and Schmidt [55] (see also [54]) using Legendre sequences. In order to state the results, we require the following notation. Let  $A$  be a sequence of length  $n$ . Let  $r$  and  $t$  be integers that can depend on  $n$ , where  $t > 0$ , and define the sequence  $A^{r,t}$  to be the sequence of length  $t$  whose  $k$ -th entry is  $A(k+r)$ , where as usual the index in  $A(k+r)$  is reduced modulo  $n$ . Informally, the sequence  $A^{r,t}$  is obtained from  $A$  by cyclically permuting (shifting) the sequence elements through  $r$  positions,

and then truncating when  $t < n$  or periodically extending (appending) when  $t > n$ . For example, if  $A = (1, 1, -1)$ , then  $A^{1,4} = (1, -1, 1, 1)$ .

Define the function  $g : \mathbb{R} \times \mathbb{R}^+ \rightarrow \mathbb{R}$  by

$$\frac{1}{g(R, T)} = 1 - \frac{4T}{3} + 4 \sum_{m \in \mathbb{N}} \max \left( 0, 1 - \frac{m}{T} \right)^2 + \sum_{m \in \mathbb{Z}} \max \left( 0, 1 - \left| 1 + \frac{2R - m}{T} \right| \right)^2,$$

where  $\mathbb{N}$  is the set of positive integers.

**Theorem 3.5.5** ([55]). *Let  $X_p$  be the Legendre sequence of length  $p$  and let  $R$  and  $T > 0$  be real. If  $r/p \rightarrow R$  and  $t/p \rightarrow T$  as  $p \rightarrow \infty$ , then  $F(X_p^{r,t}) \rightarrow g(R, T)$  as  $p \rightarrow \infty$ .*

The case  $T = 1$  of Theorem 3.5.5 implies that  $X_p^{r,p}$  has asymptotic merit factor  $g(R, 1)$  if  $r/p \rightarrow R$  as  $p \rightarrow \infty$ . Since

$$\frac{1}{g(R, 1)} = \frac{1}{6} + 8 \left( |R| - \frac{1}{4} \right)^2 \quad \text{for } |R| \leq \frac{1}{2},$$

the maximum asymptotic merit factor that can be attained in this way is  $g(1/4, 1) = 6$ . This recovers the result by Høholdt and Jensen [49], which was mentioned above.

The function  $g$  satisfies  $g(R, T) = g(R + 1/2, T)$  on its entire domain. As shown in [55, Corollary 3.2], the global maximum of  $g(R, T)$  exists and equals

$$(3.10) \quad 6.342061 \dots, \text{ the largest root of } 29x^3 - 249x^2 + 417x - 27.$$

The global maximum is unique for  $R \in [0, 1/2)$ , and is attained when  $T = 1.057827 \dots$  is the middle root of  $4x^3 - 30x + 27$  and  $R = 3/4 - T/2$ . We therefore obtain the following consequence of Theorem 3.5.5.

**Corollary 3.5.6** ([55]). *There exist binary sequences  $B_1, B_2, \dots$  of strictly increasing length satisfying  $F(B_n) \rightarrow \mathcal{F}$  as  $n \rightarrow \infty$ , where  $\mathcal{F}$  is given in (3.10).*

Corollary 3.5.6 gives the currently best known result on the asymptotic merit factor of binary sequences. However, some numerical experiments by Baden [4] suggest strongly that (3.10) is not the value of  $\limsup_{n \rightarrow \infty} \varphi(n)$ .

Theorem 3.5.5 has been generalised in various ways. First, [54, Theorem 2.1] establishes that certain binary sequences of length  $2p$  and  $4p$  constructed from a Legendre sequence of length  $p$  have essentially the same asymptotic merit factor as Legendre sequences. Second, [54, Theorem 2.3] generalises Theorem 3.5.5 in the sense that one can include also binary sequences of composite lengths whose entries are derived from the Jacobi symbol. The third generalisation is [44, Theorem 2.3] and more far-reaching. This result considers the characteristic sequences of subsets of  $\mathbb{F}_p$  obtained by joining  $m/2$  of the  $m$  cyclotomic classes in  $\mathbb{F}_p^*$  of (even) order  $m$ , where  $p$  satisfies  $p \equiv 1 \pmod{m}$ . For  $m = 2$ , we can obtain Legendre sequences, but several other popular sequence families also arise in this way [45], [3], [20], including the characteristic sequences of Hall difference sets. The asymptotic merit factor of these sequences is determined in [44] subject to a condition involving the asymptotic behaviour of their periodic autocorrelations. This condition can be checked using cyclotomic numbers and usually imposes restrictions on the underlying prime numbers.

The asymptotic behaviour of the merit factor of sequences related to Galois and Sidelnikov sequences is also known. To state the results, we require the function  $h :$

$\mathbb{R}^+ \rightarrow \mathbb{R}$  given by

$$\frac{1}{h(T)} = 1 - \frac{2T}{3} + 4 \sum_{m \in \mathbb{N}} \max\left(0, 1 - \frac{m}{T}\right)^2.$$

**Theorem 3.5.7** ([54], [44]). *Let  $q$  take values only in the set of prime powers. Let  $Y_q$  be either a Sidelnikov or a Galois sequence of length  $q - 1$  (depending on whether  $q$  is odd or even). Let  $T > 0$  be real. If  $t/q \rightarrow T$  as  $q \rightarrow \infty$ , then  $F(Y_q^{r,t}) \rightarrow h(T)$  as  $q \rightarrow \infty$ .*

The case  $T = 1$  of Theorem 3.5.7 implies that  $Y_q^{r,q-1}$  has asymptotic merit factor  $h(1) = 3$ , which was already proved by Jensen, Jensen, and Høholdt [58] for Galois sequences. The general result was first obtained by Jedwab, Katz, and Schmidt [54] for Galois sequences and by Günther and Schmidt [44] for Sidelnikov sequences. It was also shown in [44] that the conclusion of Theorem 3.5.7 remains true if Galois sequences are replaced by the characteristic sequences of cyclic difference sets obtained using the Gordon-Mills-Welch construction (see Section 2.2).

As shown in [54], the global maximum of  $h(T)$  exists and equals

$$3.342065\dots, \text{ the largest root of } 7x^3 - 33x^2 + 33x - 3.$$

The global maximum is unique and is attained for  $T = 1.115749\dots$ , which is the middle root of  $x^3 - 12x + 12$ .

#### 4. AUTOCORRELATION OF NONBINARY SEQUENCES

In this section we study properties of periodic and aperiodic autocorrelations of  $H$ -phase sequences, which are sequences whose entries are  $H$ -th roots of unity, and more generally of *unimodular* sequences, which are sequences whose entries have unit magnitude.

##### 4.1. PERIODIC AUTOCORRELATION OF NONBINARY SEQUENCES

We have seen in Section 2.3 that it seems unlikely that there is a perfect binary sequence of length greater than 4. This prompts the question as to whether there are perfect  $H$ -phase sequences, namely  $H$ -phase sequences whose nontrivial periodic autocorrelations are all zero, for larger lengths and some  $H > 2$ . We shall see that perfect  $H$ -phase sequences do exist for all lengths if we allow  $H$  to grow with the length.

Indeed, Mow [79] proposed the following generalisation of Conjecture 2.3.1.

**Conjecture 4.1.1** ([79]). *Let  $n$  be an integer with  $n > 1$  and square-free part  $r$ . Then a perfect  $H$ -phase sequence of length  $n$  exists if and only if  $H$  is divisible by*

$$\begin{cases} 2\sqrt{rn} & \text{for } n \equiv 2 \pmod{4} \\ \sqrt{rn} & \text{otherwise.} \end{cases}$$

A perfect  $n$ -phase sequence of length  $n$  is equivalent to a so-called *generalised bent function* on  $\mathbb{Z}_n$ , as studied extensively by Kumar, Scholtz, and Welch [60]. In particular, some partial proofs for both directions of Conjecture 4.1.1 are given in [60]. Most notably, [60, Property 6] shows that no perfect  $n$ -phase sequence of length  $n$  exists for  $n \equiv 2 \pmod{4}$  when 2 is semiprimitive modulo  $n/2$  (see Section 2.3 for the definition of semiprimitivity). Mow [79] has proved the “if” direction of Conjecture 4.1.1. Here

we proceed in a way that is slightly different from Mow's treatment [79] and first show that it is sufficient to take  $n$  to be a prime power.

Let  $A$  and  $B$  be sequences of length  $n_1$  and  $n_2$ , respectively. We define  $A \otimes B$  to be the sequence  $C$  of length  $n_1 n_2$  defined by

$$C(k) = A(k)B(k).$$

Note that, if  $A$  is an  $H_1$ -phase sequence and  $B$  is an  $H_2$ -phase sequence, then  $A \otimes B$  is an  $H$ -phase sequence, where  $H = \text{lcm}(H_1, H_2)$ . The following result is an immediate consequence of the Chinese Remainder Theorem.

**Lemma 4.1.2.** *Let  $A$  and  $B$  be sequences of length  $n_1$  and  $n_2$  with  $\gcd(n_1, n_2) = 1$ . Then*

$$R_u(A \otimes B) = R_u(A)R_u(B)$$

*for every  $u$ . In particular, if  $A$  and  $B$  are perfect sequences, then  $A \otimes B$  is a perfect sequence of length  $n_1 n_2$ .*

We now consider perfect sequences whose length is a power of an integer (which is not necessarily prime). We distinguish the cases that the power is even or odd. For even powers, the length is a square, in which case we take a construction due to Heimiller [46] (who considered the special case where the length is  $p^2$  for prime  $p$ ) and Frank and Zadoff [32]. For some reason, it is customary to call these sequences *Frank sequences*.

**Definition 4.1.3** (Frank sequences). Let  $m$  be a positive integer. A *Frank sequence*  $A$  of length  $m^2$  is defined by

$$A(j + km) = \exp\left(\frac{2\pi i j k}{m}\right),$$

where  $j$  and  $k$  are integers satisfying  $0 \leq j, k < m$ .

We can think of a Frank sequence of length  $m^2$  as the concatenation of the rows of the  $m \times m$  matrix with entries  $e^{2\pi i j k / m}$  at positions  $(k, j)$ .

**Theorem 4.1.4** ([46], [32]). *A Frank sequence of length  $m^2$  is a perfect  $m$ -phase sequence.*

For lengths that are odd powers of an integer, we take a construction due to Milewski [76], building on earlier results due to Chu [17].

**Definition 4.1.5** (Milewski and Chu sequences). Let  $m$  be a positive integer and let  $h$  be a nonnegative integer. A *Milewski sequence*  $A$  of length  $m^{2h+1}$  is defined by

$$A(j + km^h) = \begin{cases} \exp\left(\frac{\pi i k(2j + km^h)}{m^{h+1}}\right) & \text{for even } m \\ \exp\left(\frac{\pi i k(2j + (k+1)m^h)}{m^{h+1}}\right) & \text{for odd } m, \end{cases}$$

where  $j$  and  $k$  are integers satisfying  $0 \leq j < m^h$  and  $0 \leq k < m^{h+1}$ . For  $h = 0$ , we obtain a sequence of length  $m$ , which is also called a *Chu sequence* of length  $m$ .

We can think of a Milewski sequence of length  $m^{2h+1}$  as the concatenation of the rows of the  $m^{h+1} \times m^h$  matrix with entries

$$C(k) \exp\left(\frac{2\pi i j k}{m^{h+1}}\right)$$

at positions  $(k, j)$ , where  $C$  is a Chu sequence of length  $m$ .

**Theorem 4.1.6** ([76]). *A Milewski sequence of length  $n = m^{2h+1}$  is a perfect  $H$ -phase sequence, where*

$$H = \begin{cases} 2m & \text{for } n \equiv 2 \pmod{4} \\ m^{h+1} & \text{otherwise.} \end{cases}$$

As a consequence of Lemma 4.1.2 and Theorems 4.1.4 and 4.1.6, we obtain the following result, which proves the “if” part of Conjecture 4.1.1.

**Theorem 4.1.7.** *Let  $n$  be an integer with  $n > 1$  and square-free part  $r$ . Let*

$$n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$$

*be the prime power factorisation of  $n$ . For each  $k \in \{1, 2, \dots, s\}$ , let  $A_k$  be either a Frank or a Milewski sequence of length  $p_k^{h_k}$ , depending on whether  $h_k$  is even or odd, respectively. Then  $A_1 \otimes A_2 \otimes \cdots \otimes A_s$  is a perfect  $H$ -phase sequence of length  $n$ , where*

$$H = \begin{cases} 2\sqrt{rn} & \text{for } n \equiv 2 \pmod{4} \\ \sqrt{rn} & \text{otherwise.} \end{cases}$$

Theorem 4.1.7 is essentially due to Mow [79]. We also refer to Mow [79], [80] and the references therein for more general constructions of perfect  $H$ -phase sequences.

#### 4.2. APERIODIC AUTOCORRELATION OF NONBINARY SEQUENCES

Let  $A$  be a sequence of length  $n > 1$ . As in Section 3.2, the *peak sidelobe level* of  $A$  is

$$M(A) = \max_{0 < u < n} |C_u(A)|.$$

Note that, if  $A$  is a unimodular sequence, then  $|C_{n-1}(A)| = 1$ , and so  $M(A) \geq 1$ . Accordingly, following Golomb and Scholtz [42], we define a *unimodular* Barker sequence to be a unimodular sequence  $A$  of length at least 2 with  $M(A) = 1$ . We also define an  *$H$ -phase* Barker sequence analogously. Then a 2-phase Barker sequence is a Barker sequence in the usual sense, discussed in Section 3.1. It should be noted that it is possible to distinguish  $H$ -phase Barker sequences according to other measures for the collective smallness of the aperiodic autocorrelations (see Jedwab [53, § 7] for a detailed discussion).

For fixed  $H$ , the existence problem of  $H$ -phase Barker sequences seems to be parallel to that for ordinary Barker sequences. While  $H$ -phase Barker sequences exist for small lengths (see [53, Table 1] for  $H \in \{2, 3, 4, 6, 8\}$ ), Jedwab [53] reports the nonexistence of  $H$ -phase Barker sequences of length  $n$  for  $H = 3$  and  $10 \leq n \leq 76$ , for  $H = 4$  and  $16 \leq n \leq 60$ , for  $H = 6$  and  $19 \leq n \leq 29$ , and for  $H = 8$  and  $17 \leq n \leq 25$ . These data suggest the conjecture that, for fixed  $H$ , there are only finitely many  $H$ -phase Barker sequences.

The situation seems to be completely different if we allow  $H$  to grow with  $n$ . Indeed, using the same heuristic reasoning as that leading to Conjecture 3.4.1, Ein-Dor, Kanter, and Kinzel [22] proposed a conjecture, which we summarise as follows.

**Conjecture 4.2.1** ([22]). *Let  $m_H(n)$  be the minimum peak sidelobe level over all  $H$ -phase sequences of length  $n$ . Then*

$$\lim_{n \rightarrow \infty} m_H(n) = 1.$$

On the other hand, using clever optimisation methods, the following is known (see Nunn and Coxson [88] for latest results).

**Proposition 4.2.2.** *There exist unimodular Barker sequences for all lengths  $n \leq 70$  and for  $n \in \{72, 76, 77\}$ .*

It seems likely that Proposition 4.2.2 will be improved with the availability of more computing power. Indeed it seems plausible that unimodular Barker sequences exist for all lengths.

**Question 4.2.3.** *Is there a unimodular Barker sequence for every length?*

We now consider the aperiodic autocorrelations of specific families of unimodular sequences, namely Frank and Chu sequences (see Definitions 4.1.3 and 4.1.5). Turyn [109] calculated the peak sidelobe level of Frank sequences.

**Theorem 4.2.4** ([109]). *Let  $A_n$  be a Frank sequence of length  $n = m^2$ . Then*

$$M(A_n) = \begin{cases} 1/\sin\left(\frac{\pi}{m}\right) & \text{for even } m \\ 2/\sin\left(\frac{\pi}{2m}\right) & \text{for odd } m. \end{cases}$$

*In particular,*

$$\lim_{n \rightarrow \infty} \frac{M(A_n)}{n^{1/2}} = \frac{1}{\pi} = 0.31830 \dots$$

Theorem 4.2.4 shows that there exists an infinite family of unimodular sequences of length  $n$  whose peak sidelobe level grows like a constant times  $\sqrt{n}$ . So far, this has not been proven for binary sequences (see Section 3.4).

The asymptotic behaviour of the peak sidelobe level of Chu sequences is similar to that of Frank sequences, as shown by Mow and Li [81], although the leading constant is slightly larger.

**Theorem 4.2.5** ([81]). *Let  $A_n$  be a Chu sequence of length  $n$ . Then*

$$\lim_{n \rightarrow \infty} \frac{M(A_n)}{n^{1/2}} = \frac{\sin \sigma}{\sqrt{\pi \sigma}} = 0.48026 \dots,$$

*where  $\sigma = 1.16556 \dots$  is the smallest positive root of  $\tan x = 2x$ .*

Mow and Li [81] also give an upper bound for the peak sidelobe level of Chu sequences of length  $n$  that holds for each  $n \geq 2$ .

We conclude this section with some results on the merit factor of families of unimodular sequences. Recall from Section 3.5 that the *merit factor* of a sequence  $A$  of length  $n$  is

$$F(A) = \frac{C_0(A)^2}{2 \sum_{0 < u < n} |C_u(A)|^2},$$

provided that the denominator is nonzero.

The merit factor of Chu sequences has been studied since at least 1961 by complex analysts, including Littlewood [67], [68], [69], [70] and Newman [83]. Independently, the problem was studied in the engineering literature [2], [106], [74]. However the exact asymptotic behaviour of the merit factor of Chu sequences has only been established recently by the author [99], correcting a false calculation by Littlewood [69].



**Theorem 4.2.6** ([99]). *Let  $A_n$  be a Chu sequence of length  $n$ . Then*

$$\lim_{n \rightarrow \infty} \frac{F(A_n)}{n^{1/2}} = \frac{\pi}{2} = 1.57079 \dots$$

A stronger version of Theorem 4.2.6 has been suggested previously by Borwein and Choi [10].

**Conjecture 4.2.7** ([10]). *Let  $A_n$  be a Chu sequence of length  $n$ . Then*

$$\frac{n^{1/2}}{F(A_n)} = \frac{2}{\pi} + \frac{\delta_n}{3n} + O(n^{-2}),$$

where  $\delta_n = -2$  for  $n \equiv 0, 1 \pmod{4}$  and  $\delta_n = 1$  for  $n \equiv 2, 3 \pmod{4}$ .

The asymptotic behaviour of the merit factor of Frank sequences is also known, showing that Frank sequences are slightly better than Chu sequences with respect to the asymptotic merit factor.

**Theorem 4.2.8** ([99]). *Let  $A_n$  be a Frank sequence of square length  $n$ . Then*

$$\lim_{n \rightarrow \infty} \frac{F(A_n)}{n^{1/2}} = \frac{\pi^2}{4} = 2.46740 \dots$$

Theorem 4.2.6 and 4.2.8 show that the merit factor of unimodular sequences can grow without bound, which has not been proven so far for binary sequences.

It should be noted that the asymptotic behaviour of the peak sidelobe level and the merit factor of general Milewski sequences is currently unknown.

## 5. GOLAY PAIRS

### 5.1. DEFINITIONS AND A RECURSIVE CONSTRUCTION

In this section we study pairs of sequences  $(A, B)$  of equal length  $n$  with the property

$$C_u(A) + C_u(B) = 0 \quad \text{for all } 0 < u < n.$$

Such a pair is called a *Golay (complementary) pair*. An nontrivial example of a Golay pair is given by the two sequences

$$(1, 1, 1, -1) \quad \text{and} \quad (1, 1, -1, 1).$$

Golay introduced these objects in 1951 [36] for applications in spectrometry and studied them more systematically in 1961 [37]. Since then, Golay pairs have found many other applications, including coded aperture imaging [89] (where Golay pairs have been rediscovered and called *pinhole codes*), optical time domain reflectometry [82], medical ultrasound [86], and multicarrier communications [91], [18]. In particular, the latter application has revived the interest in Golay pairs in the last 15 years.

The central question concerning Golay pairs is: For which lengths do Golay pairs consisting of sequences with entries from a given set exist? We shall study this problem for the most important cases of *H-phase Golay pairs*, by which we mean that the two sequences in the pair are *H-phase* sequences. As usual, 2-phase Golay pairs are also called *binary* Golay pairs. For applications in multicarrier communications it is also important to know how many Golay pairs exist for a given length with entries from a given set, but we do not consider this problem here.

It is surprisingly easy to construct Golay pairs, even *binary* Golay pairs, for infinitely many lengths. Turyn [113, Lemma 5] provided a simple recursive construction that produces a Golay pair of length  $mn$  from two Golay pairs of length  $m$  and  $n$ .

**Theorem 5.1.1** ([113]). *Let  $\otimes$  be the Kronecker product and, for a sequence  $A$ , write  $A^*$  for the sequence obtained by reading  $A$  backwards. Let  $(A, B)$  be a Golay pair of length  $n$  and let  $(X, Y)$  be a binary Golay pair of length  $m$ . Then the two sequences*

$$A \otimes \left( \frac{X+Y}{2} \right) + B \otimes \left( \frac{X-Y}{2} \right) \quad \text{and} \quad A \otimes \left( \frac{X^*-Y^*}{2} \right) - B \otimes \left( \frac{X^*+Y^*}{2} \right)$$

*form a Golay pair of length  $mn$ .*

The special case that  $X = (1, 1)$  and  $Y = (1, -1)$  in Theorem 5.1.1 was previously recognised by Golay [36], [37]. In this case, Theorem 5.1.1 produces the Golay pair consisting of the sequences

$$(A, B) \quad \text{and} \quad (A, -B).$$

This is reminiscent of the recursion (3.9) that generates the Shapiro sequences. The Shapiro sequences can indeed be recovered by applying Theorem 5.1.1 iteratively to  $A = B = (1)$ . It should also be noted that Theorem 5.1.1 has several variations [29], all of which can be generalised to an array construction, which gives further Golay pairs (of the same lengths as those produced by Theorem 5.1.1) via a three-stage construction process [30].

In the next two sections we summarise the knowledge on the existence question for binary and  $H$ -phase Golay pairs.

## 5.2. BINARY GOLAY PAIRS

Binary Golay pairs are known for lengths 2, 10, and 26, for example:

$$\begin{aligned} n = 2 : & \quad (+ +) \\ & \quad (+ -) \\ n = 10 : & \quad (+ + - + - + - - + +) \\ & \quad (+ + - + + + + - -) \\ n = 26 : & \quad (+ + + + - + + - - + - + - - + - + + + - - + + +) \\ & \quad (+ + + + - + + - - + - + + + + - + - - - + + - - -) \end{aligned}$$

Interestingly, as shown by Jedwab and Parker [56], these Golay pairs can be obtained from Barker sequences of odd length. By applying Theorem 5.1.1 to these pairs, we obtain the following result.

**Corollary 5.2.1.** *There exist binary Golay pairs for all lengths of the form  $2^a 10^b 26^c$ , where  $a$ ,  $b$ , and  $c$  are nonnegative integers.*

There is a particularly nice construction by Davis and Jedwab [18, Theorem 3] for binary Golay pairs of length a power of 2.

**Theorem 5.2.2** ([18]). *Let  $m$  be a positive integer, let  $\pi$  be a permutation of  $\{1, 2, \dots, m\}$ , and let  $e, e', e_1, \dots, e_m \in \{0, 1\}$ . Define the sequences  $A$  and  $B$  of length  $2^m$  by*

$$\begin{aligned} A(j_1 + 2j_2 + \dots + 2^{m-1}j_m) &= (-1)^{\sum_{k=1}^{m-1} j_{\pi(k)}j_{\pi(k+1)} + \sum_{k=1}^m e_k j_k + e} \\ B(j_1 + 2j_2 + \dots + 2^{m-1}j_m) &= (-1)^{j_{\pi(1)} + e'} A(j_1 + 2j_2 + \dots + 2^{m-1}j_m), \end{aligned}$$

where  $j_1, \dots, j_m \in \{0, 1\}$ . Then  $(A, B)$  is a binary Golay pair.

In the case that  $\pi$  sends  $k$  to  $m + 1 - k$  in Theorem 5.2.2, we can again obtain the Shapiro sequences. Theorem 5.2.2 implies the following result [18, Corollary 5].

**Corollary 5.2.3** ([18]). *There exist at least  $2^{m+2}m!$  ordered binary Golay pairs of length  $2^m$ .*

No binary Golay pair is known whose length is not of the form  $2^a 10^b 26^c$  and no such Golay pair exists for lengths up to 100, as shown by Borwein and Ferguson [13] using clever exhaustive search methods.

**Question 5.2.4.** *Is there a binary Golay pair whose length is not of the form  $2^a 10^b 26^c$  for some nonnegative integers  $a, b, c$ ?*

It seems unlikely that Question 5.2.4 has a positive answer. Only two general results on the nonexistence of binary Golay pairs are known. The first is due to Golay himself [37] and the second is due to Eliahou, Kervaire, and Saffari [24].

**Proposition 5.2.5** ([37]). *If there exists a binary Golay sequence pair of length  $n > 1$ , then  $n$  is even.*

**Proposition 5.2.6** ([24]). *If there exists a binary Golay sequence pair of length  $n > 1$ , then  $n$  has no prime factor congruent to 3 modulo 4.*

A considerably simpler proof of Proposition 5.2.6 was later provided by Eliahou, Kervaire, and Saffari [25]. In fact, [25, Lemma 1.5] contains the following more general result, from which Proposition 5.2.6 follows immediately.

**Theorem 5.2.7** ([25]). *Let  $p$  be an odd prime and suppose that  $A, B \in \mathbb{Z}[z]$  are polynomials satisfying*

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) \equiv 0 \pmod{p}$$

*in  $\mathbb{Z}[z, z^{-1}]$ . Then  $p$  is congruent to 1 modulo 4.*

### 5.3. NONBINARY GOLAY PAIRS

We now summarise results on the existence pattern of  $H$ -phase Golay pairs. Since no two  $H$ -th roots of unity can sum to zero when  $H$  is odd, we see that  $H$ -phase Golay pairs can only exist for even  $H$ . There exist 4-phase Golay pairs of length 3, 5, 11, and 13 [33], [51]. As shown by Gibson and Jedwab [35], these can also be obtained from Barker sequences of odd length. It then follows from Theorem 5.1.1 and Corollary 5.2.1 that there exist 4-phase Golay pairs for all lengths of the form

$$(5.1) \quad 2^a 10^b 26^c m, \text{ where } a, b, c \geq 0 \text{ are integers and } m \in \{1, 3, 5, 11, 13\}.$$

No  $H$ -phase Golay pair is known whose length is not of the form (5.1), although there are 6-phase Golay pairs of length a multiple of 10 [28] or a multiple of 16 [31], [28] that are not (and cannot be trivially obtained from) binary Golay pairs. The smallest natural numbers not of the form (5.1) are 7, 9, 14, and 15, and indeed, it has been verified with a computer [28] that there is no  $H$ -phase Golay pair of length  $n$  for  $n \in \{7, 9\}$  and all  $H \leq 36$  and for  $n \in \{14, 15\}$  and all  $H \leq 10$ .

**Question 5.3.1.** *Is there an  $H$ -phase Golay pair whose length is not of the form (5.1)? In particular, is there an  $H$ -phase Golay pair of odd length  $n > 13$ ?*

From Proposition 5.2.5 we know that there is no binary Golay pair of odd length  $n > 1$ . Fiedler [28, Conjecture 1] conjectured the more general assertion that there is no  $H$ -phase Golay pair of odd length  $n > 1$  whenever  $H \equiv 2 \pmod{4}$ .

**Conjecture 5.3.2** ([28]). *If  $H \equiv 2 \pmod{4}$ , then there is no  $H$ -phase Golay pair of odd length  $n > 1$ .*

Conjecture 5.3.2 holds for values of  $H$  having a small odd prime divisor, which can be deduced from the following result [28, Corollary 5.2].

**Proposition 5.3.3** ([28]). *Let  $H > 2$  be an integer satisfying  $H \equiv 2 \pmod{4}$  and let  $p$  be the smallest odd prime factor of  $H$ . If there exists an  $H$ -phase Golay pair of odd length  $n$ , then  $n < 2p$ .*

For example, there is no 6-phase Golay pair of odd length greater than 6. The nonexistence of 6-phase Golay pairs of length 3 and 5 is easily established, so the assertion of Conjecture 5.3.2 is true for  $H = 6$ . Similarly, the assertion of Conjecture 5.3.2 is true for all  $H \leq 36$  [28].

Fiedler [28] also proved the following result, which crucially relies on Theorem 5.2.7 and complements Proposition 5.2.6.

**Proposition 5.3.4** ([28]). *Let  $p$  be an odd prime congruent to 3 modulo 4 and let  $H$  be twice a power of  $p$ . If there exists an  $H$ -phase Golay pair of length  $n$ , then  $p$  does not divide  $n$ .*

For example, there are no 6-phase Golay pairs of lengths 3, 6, 9, 12, . . . .

#### ACKNOWLEDGEMENTS

I would like to thank Christian Günther, Jonathan Jedwab, Dieter Jungnickel, and Peter Wild for some careful comments on a draft of this survey.

#### REFERENCES

- [1] N. Alon, S. Litsyn, and A. Shpunt. Typical peak sidelobe level of binary sequences. *IEEE Trans. Inform. Theory*, 56(1):545–554, 2010.
- [2] M. Antweiler and L. Bömer. Merit factor of Chu and Frank sequences. *IEE Electron. Lett.*, 46(25):2068–2070, 1990.
- [3] K. T. Arasu, C. Ding, T. Hellesteth, P. V. Kumar, and H. M. Martinsen. Almost difference sets and their sequences with optimal autocorrelation. *IEEE Trans. Inform. Theory*, 47(7):2934–2943, 2001.
- [4] J. M. Baden. Efficient optimization of the merit factor of long binary sequences. *IEEE Trans. Inform. Theory*, 57(12):8084–8094, 2011.
- [5] R. H. Barker. Group synchronization of binary digital systems. In W. Jackson, editor, *Communication Theory*, pages 173–187. Academic Press, New York, 1953.
- [6] G. F. M. Beenker, T. A. C. M. Claasen, and P. W. C. Hermens. Binary sequences with a maximally flat amplitude spectrum. *Philips J. Res.*, 40(5):289–304, 1985.
- [7] J. Bernasconi. Low autocorrelation binary sequences: statistical mechanics and configuration state analysis. *J. Physique*, 48(4):559–567, 1987.
- [8] A. M. Boehmer. Binary pulse compression codes. *IEEE Trans. Inform. Theory*, IT-13(2):156–167, 1967.
- [9] P. Borwein. *Computational excursions in analysis and number theory*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 10. Springer-Verlag, New York, 2002.
- [10] P. Borwein and K.-K. S. Choi. Merit factors of character polynomials. *J. London Math. Soc.*, 61:706–720, 2000.

- [11] P. Borwein and M. Mossinghoff. Rudin-Shapiro-like polynomials in  $L_4$ . *Math. Comp.*, 69(231):1157–1166, 2000.
- [12] P. Borwein and M. J. Mossinghoff. Wieferich pairs and Barker sequences, II. *LMS J. Comput. Math.*, 17(1):24–32, 2014.
- [13] P. B. Borwein and R. A. Ferguson. A complete description of Golay pairs for lengths up to 100. *Math. Comp.*, 73(246):967–985, 2004.
- [14] A. Brauer. On a new class of Hadamard determinants. *Math. Z.*, 58:219–225, 1953.
- [15] W. J. Broughton. A note on Table I of: “Barker sequences and difference sets”. *Enseign. Math. (2)*, 40(1-2):105–107, 1994.
- [16] Y. Cai and C. Ding. Binary sequences with optimal autocorrelation. *Theoret. Comput. Sci.*, 410(24-25):2316–2322, 2009.
- [17] D. Chu. Polyphase codes with good periodic correlation properties. *IEEE Trans. Inform. Theory*, IT-18(4):531–532, 1972.
- [18] J. A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Trans. Inform. Theory*, 45(7):2397–2417, 1999.
- [19] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields Appl.*, 10(3):342–389, 2004.
- [20] C. Ding, T. Hellese, and K. Y. Lam. Several classes of binary sequences with three-level autocorrelation. *IEEE Trans. Inform. Theory*, 45(7):2606–2612, 1999.
- [21] D. Dmitriev and J. Jedwab. Bounds on the growth rate of the peak sidelobe level of binary sequences. *Adv. Math. Commun.*, 1(4):461–475, 2007.
- [22] L. Ein-Dor, I. Kanter, and W. Kinzel. Low autocorrelated multiphase sequences. *Phys. Rev. (E)*, 65(2):020102.1–020102.4, 2002.
- [23] Sh. Eliahou and M. Kervaire. Barker sequences and difference sets. *Enseign. Math. (2)*, 38(3-4):345–382, 1992.
- [24] Sh. Eliahou, M. Kervaire, and B. Saffari. A new restriction on the lengths of Golay complementary sequences. *J. Combin. Theory Ser. A*, 55(1):49–59, 1990.
- [25] Sh. Eliahou, M. Kervaire, and B. Saffari. On Golay polynomial pairs. *Adv. Appl. Math.*, 12(3):235–292, 1991.
- [26] P. Erdős. Some old and new problems in approximation theory: research problems 95-1. *Constr. Approx.*, 11(3):419–421, 1995.
- [27] R. Evans, H. D. L. Hollmann, Ch. Krattenthaler, and Q. Xiang. Gauss sums, Jacobi sums, and  $p$ -ranks of cyclic difference sets. *J. Combin. Theory Ser. A*, 87(1):74–119, 1999.
- [28] F. Fiedler. Small Golay sequences. *Adv. Math. Commun.*, 7(4):379–407, 2013.
- [29] F. Fiedler, J. Jedwab, and M. G. Parker. A framework for the construction of Golay sequences. *IEEE Trans. Inform. Theory*, 54(7):3114–3129, 2008.
- [30] F. Fiedler, J. Jedwab, and M. G. Parker. A multi-dimensional approach to the construction and enumeration of Golay complementary sequences. *J. Combin. Theory Ser. A*, 115(5):753–776, 2008.
- [31] F. Fiedler, J. Jedwab, and A. Wiebe. A new source of seed pairs for Golay sequences of length  $2^m$ . *J. Combin. Theory Ser. A*, 117(5):589–597, 2010.
- [32] R. Frank and S. Zadoff. Phase shift pulse codes with good periodic correlation properties. *IRE Trans. Inform. Theory*, IT-8(6):381–382, 1962.
- [33] R. L. Frank. Polyphase complementary codes. *IEEE Trans. Inform. Theory*, 26(6):641–647, 1980.
- [34] M. L. Fredman, B. Saffari, and B. Smith. Polynômes réciproques: conjecture d’Erdős en norme  $L^4$ , taille des autocorrélations et inexistence des codes de Barker. *C. R. Acad. Sci. Paris Sér. I Math.*, 308(15):461–464, 1989.
- [35] R. G. Gibson and J. Jedwab. Quaternary Golay sequence pairs II: odd length. *Des. Codes Cryptogr.*, 59(1-3):147–157, 2011.
- [36] M. J. E. Golay. Static multislit spectrometry and its applications to the panoramic display of infrared spectra. *J. Opt. Soc. Amer.*, 41:468–472, 1951.
- [37] M. J. E. Golay. Complementary series. *IRE Trans. Inform. Theory*, IT-7(2):82–87, 1961.
- [38] M. J. E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory*, IT-18(3):449–450, 1972.
- [39] M. J. E. Golay. The merit factor of long low autocorrelation binary sequences. *IEEE Trans. Inform. Theory*, 28(3):543–549, 1982.

- [40] S. W. Golomb. *Shift register sequences*. Holden-Day, Inc., San Francisco, Calif.-Cambridge-Amsterdam, 1967.
- [41] S. W. Golomb and G. Gong. *Signal design for good correlation*. Cambridge University Press, Cambridge, 2005. For wireless communication, cryptography, and radar.
- [42] S. W. Golomb and R. A. Scholtz. Generalized Barker sequences. *IEEE Trans. Inform. Theory*, IT-11(4):533–537, 1965.
- [43] B. Gordon, W. H. Mills, and L. R. Welch. Some new difference sets. *Canad. J. Math.*, 14:614–625, 1962.
- [44] Ch. Günther and K.-U. Schmidt. Merit factors of polynomials derived from difference sets. arXiv:1503.05858 [math.CO].
- [45] M. Hall Jr. A survey of difference sets. *Proc. Amer. Math. Soc.*, 7:975–986, 1956.
- [46] R. C. Heimiller. Phase shift pulse codes with good periodic correlation properties. *IRE Trans. Inform. Theory*, IT-7(4):254–257, 1961.
- [47] T. Høholdt and P. V. Kumar. Sequences with low correlation. In *Handbook of coding theory, Vol. II*, pages 1765–1853. North-Holland, Amsterdam, 1998.
- [48] T. Høholdt. The merit factor problem for binary sequences. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 3857 of *Lecture Notes in Comput. Sci.*, pages 51–59. Springer, Berlin, 2006.
- [49] T. Høholdt and H. E. Jensen. Determination of the merit factor of Legendre sequences. *IEEE Trans. Inform. Theory*, 34(1):161–164, 1988.
- [50] T. Høholdt, H. E. Jensen, and J. Justesen. Aperiodic correlations and the merit factor of a class of binary sequences. *IEEE Trans. Inform. Theory*, 31(4):549–552, 1985.
- [51] W. H. Holzmann and H. Kharaghani. A computer search for complex Golay sequences. *Australas. J. Combin.*, 10:251–258, 1994.
- [52] J. Jedwab. A survey of the merit factor problem for binary sequences. In *Proc. of Sequences and Their Applications*, volume 3486 of *Lecture Notes in Comput. Sci.*, pages 30–55. New York: Springer Verlag, 2005.
- [53] J. Jedwab. What can be used instead of a Barker sequence? *Contemp. Math.*, 461:153–178, 2008.
- [54] J. Jedwab, D. J. Katz, and K.-U. Schmidt. Advances in the merit factor problem for binary sequences. *J. Combin. Theory Ser. A*, 120(4):882–906, 2013.
- [55] J. Jedwab, D. J. Katz, and K.-U. Schmidt. Littlewood polynomials with small  $L^4$  norm. *Adv. Math.*, 241:127–136, 2013.
- [56] J. Jedwab and M. G. Parker. A construction of binary Golay sequence pairs from odd-length Barker sequences. *J. Combin. Des.*, 17(6):478–491, 2009.
- [57] J. Jedwab and K. Yoshida. The peak sidelobe level of families of binary sequences. *IEEE Trans. Inform. Theory*, 52(5):2247–2254, 2006.
- [58] J. M. Jensen, H. E. Jensen, and T. Høholdt. The merit factor of binary sequences related to difference sets. *IEEE Trans. Inform. Theory*, 37(3):617–626, 1991.
- [59] D. Jungnickel and A. Pott. Perfect and almost perfect sequences. *Discrete Appl. Math.*, 95(1-3):331–359, 1999.
- [60] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *J. Combin. Theory Ser. A*, 40(1):90–107, 1985.
- [61] E. S. Lander. *Symmetric designs: an algebraic approach*, volume 74 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.
- [62] A. Lempel, M. Cohn, and W. L. Eastman. A class of balanced binary sequences with optimal autocorrelation properties. *IEEE Trans. Inform. Theory*, IT-23(1):38–42, 1977.
- [63] A. N. Leukhin and E. N. Potekhin. Exhaustive search for optimal minimum peak sidelobe binary sequences up to length 80. In *Sequences and Their Applications*, volume 8865 of *Lecture Notes in Comput. Sci.*, pages 157–169. Springer, 2014.
- [64] K. H. Leung and B. Schmidt. The field descent method. *Des. Codes Cryptogr.*, 36(2):171–188, 2005.
- [65] K. H. Leung and B. Schmidt. New restrictions on possible orders of circulant Hadamard matrices. *Des. Codes Cryptogr.*, 64(1-2):143–151, 2012.
- [66] K. H. Leung and B. Schmidt. The anti-field-descent method, 2015. Preprint available at <http://www3.ntu.edu.sg/home/bernhard/Publications/publications.html>.

- [67] J. E. Littlewood. On the mean values of certain trigonometric polynomials. *J. London Math. Soc.*, 36:307–334, 1961.
- [68] J. E. Littlewood. On the mean values of certain trigonometric polynomials II. *Illinois J. Math.*, 6:1–39, 1962.
- [69] J. E. Littlewood. On polynomials  $\sum^n \pm z^m$ ,  $\sum^n e^{\alpha m i} z^m$ ,  $z = e^{\theta i}$ . *J. London Math. Soc.*, 41(1):367–376, 1966.
- [70] J. E. Littlewood. *Some problems in real and complex analysis*. D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.
- [71] B. Logan and M. J. Mossinghoff. Double Wieferich pairs and circulant Hadamard matrices, 2015. Preprint available at <http://academics.davidson.edu/math/mossinghoff/>.
- [72] A. Maschietti. Difference sets and hyperovals. *Des. Codes Cryptogr.*, 14(1):89–98, 1998.
- [73] Ch. Mauduit and A. Sárközy. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. *Acta Arith.*, 82(4):365–377, 1997.
- [74] I. Mercer. Merit factor of Chu sequences and best merit factor of polyphase sequences. *IEEE Trans. Inform. Theory*, 59(9):6083–6086, 2013.
- [75] I. D. Mercer. Autocorrelations of random binary sequences. *Combin. Probab. Comput.*, 15(5):663–671, 2006.
- [76] A. Milewski. Periodic sequences with optimal properties for channel estimation and fast start-up equalization. *IBM J. Res. Develop.*, 27(5):426–431, 1983.
- [77] J. W. Moon and L. Moser. On the correlation function of random binary sequences. *SIAM J. Appl. Math.*, 16(12):340–343, 1968.
- [78] M. J. Mossinghoff. Wieferich pairs and Barker sequences. *Des. Codes Cryptogr.*, 53(3):149–163, 2009.
- [79] W. H. Mow. A unified construction of perfect polyphase sequences. In *IEEE Int. Symp. Inform. Theory*, page 459. IEEE, 1995.
- [80] W. H. Mow. A new unified construction of perfect root-of-unity sequences. In *IEEE 4th Int. Symp. Spread Spectrum Techniques and Applications*, pages 955–959, vol.3. IEEE, 1996.
- [81] W. H. Mow and Sh-Y. R. Li. Aperiodic autocorrelation and crosscorrelation of polyphase sequences. *IEEE Trans. Inform. Theory*, 43(3):1000–1007, 1997.
- [82] M. Nazarathy, S. A. Newton, R. P. Giffard, D. S. Moberly, F. Sischka, W. R. Trutna, Jr., and S. Foster. Real-time long range complementary correlation optical time domain reflectometer. *IEEE J. Lightwave Technology*, 7(1):24–38, 1989.
- [83] D. J. Newman. An  $L^1$  extremal problem for polynomials. *Proc. Amer. Math. Soc.*, 16:1287–1290, 1965.
- [84] D. J. Newman and J. S. Byrnes. The  $L^4$  norm of a polynomial with coefficients  $\pm 1$ . *Amer. Math. Monthly*, 97:42–45, 1990.
- [85] J.-S. No, H. Chung, and M.-S. Yun. Binary pseudorandom sequences of period  $2^m - 1$  with ideal autocorrelation generated by the polynomial  $z^d + (z + 1)^d$ . *IEEE Trans. Inform. Theory*, 44(3):1278–1282, 1998.
- [86] A. Nowicki, W. Secomski, J. Litniewski, I. Trots, and P. A. Lewin. On the application of signal compression using Golay’s codes sequences in ultrasonic diagnostic. *Arch. Acoustics*, 28(4):313–324, 2003.
- [87] C. J. Nunn and G. E. Coxson. Best-known autocorrelation peak sidelobe levels for binary codes of length 71 to 105. *IEEE Trans. Aerosp. Electron. Sys.*, 44(4):392–395, 2008.
- [88] C. J. Nunn and G. E. Coxson. Polyphase pulse compression codes with optimal peak and integrated sidelobes. *IEEE Trans. Aerosp. Electron. Sys.*, 45(2):775–781, 2009.
- [89] N. Ohyama, T. Honda, and J. Tsujiuchi. An advanced coded imaging without side lobes. *Optics Commun.*, 27(3):339–344, 1978.
- [90] R.E.A.C. Paley. On orthogonal matrices. *J. Math. Phys.*, 12:311–320, 1933.
- [91] B. M. Popović. Synthesis of power efficient multitone signals with flat amplitude spectrum. *IEEE Trans. Commun.*, 39(7):1031–1033, 1991.
- [92] W. Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959.
- [93] H. J. Ryser. *Combinatorial mathematics*. The Carus Mathematical Monographs, No. 14. Published by The Mathematical Association of America; distributed by John Wiley and Sons, Inc., New York, 1963.

- [94] D. V. Sarwate. An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. *IEEE Trans. Inform. Theory*, IT-30(4):685–687, 1984.
- [95] B. Schmidt. Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.*, 12(4):929–952, 1999.
- [96] B. Schmidt. *Characters and cyclotomic fields in finite geometry*, volume 1797 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.
- [97] K.-U. Schmidt. Binary sequences with small peak sidelobe level. *IEEE Trans. Inform. Theory*, 58(4):2512–2515, 2012.
- [98] K.-U. Schmidt. On random binary sequences. In *Sequences and Their Applications*, volume 7280 of *Lecture Notes in Comput. Sci.*, pages 303–314. Springer, 2012.
- [99] K.-U. Schmidt. On a problem due to Littlewood concerning polynomials with unimodular coefficients. *J. Fourier Anal. Appl.*, 19(3):457–466, 2013.
- [100] K.-U. Schmidt. The peak sidelobe level of random binary sequences. *Bull. London Math. Soc.*, 46(3):643–652, 2014.
- [101] K.-U. Schmidt and J. Willms. Barker sequences of odd length. *Des. Codes. Cryptogr.* (to appear).
- [102] R. A. Scholtz and L. R. Welch. GMW sequences. *IEEE Trans. Inform. Theory*, 30(3):548–553, 1984.
- [103] H. S. Shapiro. Extremal problems for polynomials and power series. Master’s thesis, MIT, 1951.
- [104] V. M. Sidelnikov. Some  $k$ -valued pseudo-random sequences and nearly equidistant codes. *Probl. Inform. Transm.*, 5:12–16, 1969.
- [105] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938.
- [106] S. Stańczak and H. Boche. Aperiodic properties of generalized binary Rudin-Shapiro sequences and some recent results on sequences with a quadratic phase function. In *Proc. of International Zurich Seminar on Broadband Communications*, pages 279–286. IEEE, 2000.
- [107] R. Turyn. Optimum codes study. Technical report, Sylvania Electronic Systems, January 1960. Final report, Contract AF19(604)-5473.
- [108] R. Turyn. On Barker codes of even length. *Proceedings of the IEEE*, 51(9):1256–1256, 1963.
- [109] R. Turyn. The correlation function of a sequences of roots of 1. *IEEE Trans. Inform. Theory*, IT-13(3):524–525, 1967.
- [110] R. Turyn and J. Storer. On binary sequences. *Proc. Amer. Math. Soc.*, 12(3):394–399, 1961.
- [111] R. J. Turyn. Character sums and difference sets. *Pacific J. Math.*, 15(1):319–346, 1965.
- [112] R. J. Turyn. Sequences with small correlation. In Henry B. Mann, editor, *Error Correcting Codes*. Wiley, New York, 1968.
- [113] R. J. Turyn. Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. *J. Combin. Theory Ser. A*, 16:313–333, 1974.

DEPARTMENT OF MATHEMATICS, PADERBORN UNIVERSITY, WARBURGER STR. 100, 33098 PADERBORN, GERMANY

*E-mail address:* kus@math.upb.de